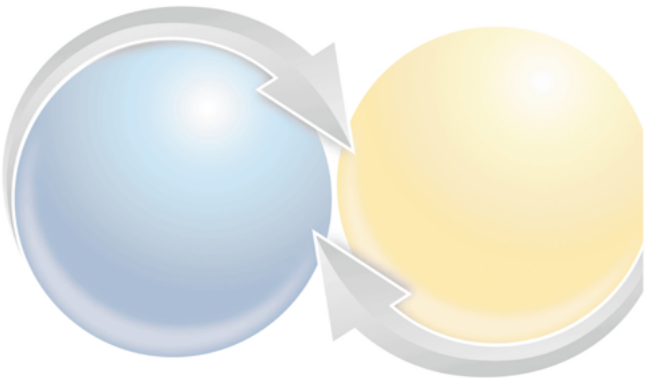
Livelink WCM Server

Administrator Manual

This manual describes how to configure and administer your WCM system with the Admin client. It provides information on the following topics:

- basic technical concepts of Livelink WCM Server
- introduction to working with the Admin client
- user administration functions
- configuring and administering WCM system elements, such as websites, servers, agents, etc.



OPEN TEXT CORPORATION

Great Minds Working Together™

Copyright 2006 by Open Text Corporation.

The copyright to these materials and any accompanying software is owned, without reservation, by Open Text Corporation. These materials and any accompanying software may not be copied in whole or part without the express, written permission of Open Text Corporation.

Open Text Corporation is the owner of the trademarks Open Text, 'Great Minds Working Together', Livelink, and MeetingZone among others. This list is not exhaustive. All other products or company names are used for identification purposes only, and are trademarks of their respective owners. All rights reserved.

Open Text Corporation provides certain warranties and limitations in connection with the software that this document describes. For information about these warranties and limitations, refer to the license agreement entered into between the licensee and Open Text Corporation.

Contacting Us

Open Text Corporation
Corporate Headquarters
275 Frank Tompa Drive,
Waterloo, Ontario, Canada
N2L 0A1

(519) 888-7111

If you subscribe to our Customer Assistance Program or would like more information about the support program, write to Open Text Corporation's Customer Support at support@opentext.com or telephone (800) 540-7292 or (519) 888-9933. Our support hours are Monday through Friday, 8:30 a.m. to 8 p.m. (EST).

If you have comments or suggestions regarding this documentation, write to the Open Text Corporation Publications Group at documentation@opentext.com.

For more information about Open Text Corporation's products and services, visit our home page at http://www.opentext.com.

© 2006 IXOS SOFTWARE AG

Werner-v.-Siemens-Ring 20
85630 Grasbrunn, Germany

Tel.: +49 (89) 4629-0
Fax: +49 (89) 4629-1199
eMail: office@ixos.de
Internet: http://www.ixos.com

All rights reserved, including those regarding reproduction, copying or other use or communication of the contents of this document or parts thereof. No part of this publication may be reproduced, transmitted to third parties, processed using electronic retrieval systems, copied, distributed or used for public demonstration in any form without the written consent of IXOS SOFTWARE AG. We reserve the right to update or modify the contents. Any and all information that appears within illustrations of screenshots is

provided coincidentally to better demonstrate the functioning of the software. IXOS SOFTWARE AG hereby declares that this information reflects no statistics of nor has any validity for any existing company. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/) and software developed by the Apache Software Foundation (http://www.apache.org/).

Trademarks IXOS: IXOS SOFTWARE AG.

SAP®, R/3® and SAP ArchiveLink® are registered trademarks of SAP AG.

Microsoft®, Microsoft Windows NT® and the names of further Microsoft products are registered trademarks of Microsoft Corporation.

Acrobat Reader Copyright © 1987 Adobe Systems Incorporated. All rights reserved. Adobe and Acrobat are trademarks of Adobe Systems Incorporated which may be registered in certain jurisdictions.

Siebel® is a registered trademark by Siebel Systems, Inc.

Other product names are used only to identify the products and they may be registered trademarks of the relevant manufacturers.

Copyright © 2006 Gauss Interprise AG Hamburg, Gauss Interprise, Inc. Irvine, California. All rights reserved worldwide.

This document and the related software are property of Gauss Interprise AG or its suppliers and protected by copyright and other laws. They are distributed under licenses restricting their use, copying, distribution, and decompilation. Neither receipt nor possession of this document confers or transfers any right to reproduce or disclose any part of the contents hereof. No part of this document may be reproduced in any form by any means without prior written authorization of Gauss Interprise AG or Gauss Interprise, Inc.

Moreover, the regulations of the software license agreement apply to this documentation.

All brand names and trademarks mentioned are the property of their respective owners.

http://www.opentext.com/bridging/gauss.html

Program version: Livelink Web Content Management Server™ (Content Server) 9.5.1

Document version: En-01

Publication date: May 2006

Table of Contents

List of Figures **8**

List of Tables **12**

Chapter 1 Introduction **15**

What Livelink WCM Server Has to Offer 15

About this Manual 19

Typographic Conventions 22

Chapter 2 Concepts **25**

Basic Components of a WCM System 25

Scenarios for Setting up a WCM System 55

Access Control 65

Unicode with Livelink WCM Server 82

WebDAV with Livelink WCM Server 87

Chapter 3 Working in the Admin Client **95**

Logging In and Out 95

The User Interface of the Admin Client 98

Editing Items in the Admin Client 102

Managing Other Products of Livelink WCM Server 115

General Settings of the Admin Client 116

Using the Admin Client as a Web Application 117

Deploying Resources 122

Help on the Admin Client 128

Chapter 4 User Administration 131
User Administration Functions 132
Setting WCM Attributes in LDAP 134
Managing Users 136
Managing Groups and Roles 143
Managing the Rights of the Principal “World” 150
Managing Functional Areas 150
Website Assignments 156

Chapter 5 Managing Pools and Connection Types 159
Adding a Pool 162
Pool Settings 164
Deleting a Pool 167
Adding a Custom Connection Type 168
Connection Types Settings 168
Deleting a Custom Connection Type 170

Chapter 6 Managing Servers 173
General Server Settings 176
Websites Assigned to Servers 177
Deployment Systems of a Server 180
Assigning Pools to Servers 182
Assigning Agents to Servers 184
Services Available on a Server 186
Managing Paths for Secure Access 186
Managing Proxy Admin Servers 189
Deleting Servers from the Configuration 197

Chapter 7	**Managing Websites**	**201**
	Creating a New Website	204
	General Website Settings	226
	Deployment Systems of a Website	227
	Proxy Content Servers Assigned to a Website	228
	Managing Object Types of Websites	229
	Managing Attribute Sets of Websites	234
	Managing Object Categories of Websites	237
	Assigning Converters to Websites	240
	Reassigning Orphan Objects	243
	Deleting a Website	245
	Exporting and Importing Websites	246
Chapter 8	**Managing Deployment Systems**	**273**
	Adding a Deployment System	275
	Settings of Deployment Systems	276
	Deleting a Deployment System	278
Chapter 9	**Managing Agents and Utilities**	**281**
	Managing Server Agents	282
	Managing Utilities	310
Chapter 10	**System Administration**	**315**
	Administering Active Servers	317
	Managing Logged-in Users	339
	Managing Active Websites	341
	Managing Licenses	344
	Data Backup	347

Chapter 11 System Overview 353

Information in the System Overview 354

Functions of the System Overview 358

Glossary 365

Index 375

List of Figures

Fig. 1 –	Simplified WCM system and its environment	27
Fig. 2 –	The staging of Livelink WCM Server	30
Fig. 3 –	Example workflow in Livelink WCM Server	31
Fig. 4 –	WCM system consisting of master and proxy Content servers	34
Fig. 5 –	Communication via VIPP and HTTP tunneling	48
Fig. 6 –	Use of SSL for VIPP and HTTP tunneling	49
Fig. 7 –	Structure of a minimum system	56
Fig. 8 –	Distributed WCM system with firewall	59
Fig. 9 –	Distributed WCM system with separate databases	61
Fig. 10 –	WCM system with two websites	64
Fig. 11 –	Access rights for Edit, QA, and Production	73
Fig. 12 –	Overview of Secure Access	80
Fig. 13 –	Configuring the JDBC pool for WebDAV	89
Fig. 14 –	Configuring multiple JDBC pools for WebDAV	90
Fig. 15 –	Logging in to the Admin client	96
Fig. 16 –	The user interface of the Admin client	98
Fig. 17 –	Icons available for a selected website	100
Fig. 18 –	Icons available for *InternetSite* → *Proxy Content servers*	100
Fig. 19 –	Context menus for a selected website and for *InternetSite* → *Proxy Content servers*	101
Fig. 20 –	Menu commands and keyboard shortcuts	102
Fig. 21 –	Website list	103
Fig. 22 –	Filter criteria for displaying users	105
Fig. 23 –	Adding an item via the context menu	106
Fig. 24 –	Basic settings of a group	108
Fig. 25 –	Assignments of a group	109
Fig. 26 –	Assignment using the context menu	110

Fig. 27 – Assigning a user to a group 111
Fig. 28 – Removing assignments using the context menu 112
Fig. 29 – Two ways to assign a server to a website 113
Fig. 30 – User assignments overview 114
Fig. 31 – Assignments for a role 115
Fig. 32 – General settings of the Admin client 116
Fig. 33 – Creating a web application for the Admin client 120
Fig. 34 – Selecting a web application for the Admin client 121
Fig. 35 – User administration items 132
Fig. 36 – Selecting LDAP principals 135
Fig. 37 – Configured users 137
Fig. 38 – Dialog box for adding a user 138
Fig. 39 – Editing user information 139
Fig. 40 – Assignments of a user 140
Fig. 41 – Groups of the WCM system 144
Fig. 42 – Dialog box for adding a group 145
Fig. 43 – Assignments of a group 147
Fig. 44 – Available functional areas 151
Fig. 45 – Dialog box for adding a functional area 152
Fig. 46 – Settings of functional areas 153
Fig. 47 – Website assignments 156
Fig. 48 – Overview of available pools and connection types 159
Fig. 49 – Settings of a pool 165
Fig. 50 – Settings of a connection type 169
Fig. 51 – Overview of installed servers 173
Fig. 52 – Settings of a server 176
Fig. 53 – Overview of websites assigned to a server 178
Fig. 54 – Overview of the deployment systems of a server 181
Fig. 55 – Overview of the pools for a server 182

Fig. 56 – Determining the sequence of the LDAP pools 184
Fig. 57 – Overview of the agents of a server 185
Fig. 58 – Settings of a path for Secure Access 188
Fig. 59 – Registering a proxy Admin server 193
Fig. 60 – Overview of managed websites 201
Fig. 61 – Assignments of a website 202
Fig. 62 – Options when creating a new website 205
Fig. 63 – Basic information for the new website 207
Fig. 64 – Initial assignment of a principal to a website 210
Fig. 65 – Specifying base URL and directory for master Content server 212
Fig. 66 – Specifying base URL, application name, and application directory for master Content server 214
Fig. 67 – Specifying names of deployment systems 216
Fig. 68 – Configuring proxy Content servers for the website 219
Fig. 69 – Overview of all selected proxy Content servers 220
Fig. 70 – Defining the routing 221
Fig. 71 – Website servers without deployment systems 222
Fig. 72 – Overview of the deployment systems for a server 223
Fig. 73 – Overview of existing deployment systems 225
Fig. 74 – Overview of the deployment systems for a website 227
Fig. 75 – Proxy Content servers assigned to a website 228
Fig. 76 – Overview of available object types 230
Fig. 77 – Default attribute sets 235
Fig. 78 – Dialog box for assigning orphan WCM objects 244
Fig. 79 – Connection parameters for the master Content server 250
Fig. 80 – Information for exporting a website 251
Fig. 81 – Information for importing a website 252
Fig. 82 – Installed deployment systems 274
Fig. 83 – Settings of deployment systems 276

Fig. 84 – Overview of available agents 283
Fig. 85 – Configuring a parameter for an agent 286
Fig. 86 – Servers assigned to an agent 287
Fig. 87 – Configuring the agent for automatic conversion 297
Fig. 88 – Adding a node to the FileLabeling agent 299
Fig. 89 – The node “objecttypes” 299
Fig. 90 – Configuring the FileLabeling agent 301
Fig. 91 – New node for LivelinkFolderSynchronization agent 303
Fig. 92 – Configuration below the website node 304
Fig. 93 – Configuration below the folder node 306
Fig. 94 – Configuring the agent for default content 309
Fig. 95 – Overview of available utilities 310
Fig. 96 – System administration items 315
Fig. 97 – Overview of active servers 317
Fig. 98 – Overview of the websites of a server 323
Fig. 99 – Changing the run level of a website 324
Fig. 100 – Reports available for a master Content server 325
Fig. 101 – Logs available for a master Content server 330
Fig. 102 – Trace log of a server 333
Fig. 103 – Overview of the actions in progress on a server 334
Fig. 104 – Status of the agents on a master Content server 335
Fig. 105 – Creating a web application for a server 338
Fig. 106 – List of logged-in users 339
Fig. 107 – Overview of active websites 341
Fig. 108 – Overview of the servers assigned to a website 344
Fig. 109 – License display in the system administration 345
Fig. 110 – The system overview items 354
Fig. 111 – Legend in system overview 355
Fig. 112 – Generating e-mail with system files 362

List of Tables

Table 1 –	Data storage views and possible deployment systems (DS)	38
Table 2 –	Functional areas and object types	69
Table 3 –	The individual administration rights	75
Table 4 –	Functions in the four Admin client tabs	99
Table 5 –	Configuration items that can be localized	125
Table 6 –	Items and functions of the user administration	132
Table 7 –	Server assignments	174
Table 8 –	Assignments of websites	202
Table 9 –	Entries in the **export-import-conf.xml** file	254
Table 10 –	Entries in the file **subtree-export-import-conf.xml**	265
Table 11 –	Functions for the configuration of server agents and utilities	281
Table 12 –	Overview of the server agents supplied	289
Table 13 –	Log parameters for the FileLabeling agent	300
Table 14 –	Utilities and their functions	311
Table 15 –	Items and functions of the system administration	316
Table 16 –	Server run levels	319
Table 17 –	Website run levels	342
Table 18 –	System overview items	356
Table 19 –	Icons and functions in the *System overview*	358

CHAPTER 1
Introduction

This chapter gives you an introduction to the functionality of Livelink Web Content Management Server™ (Livelink WCM Server for short). It also provides a brief overview of the structure of this documentation.

What Livelink WCM Server Has to Offer

Many companies today have a number of intranet, extranet, and Internet environments with specific focuses. This involves managing content for a wide variety of target groups: employees, subsidiaries, business associates, or customers. An efficient content management system in the company makes it possible to equip users with the rights and tools they need to provide such content, and at the same time ensure control of the content.

Livelink WCM Server enables you to implement sophisticated intranet and Internet solutions. The content is managed in the form of complex websites. Livelink WCM Server includes other products for creating and managing dynamic and personalized websites. Together with other WCM components such as the Portal Manager API, Livelink WCM Server ensures the provision of static and dynamic content in enterprise portals, intranet and Internet solutions. Livelink WCM Server coordinates the tasks of compiling and distributing company-relevant content, and covers its entire life cycle – from content creation through quality assurance, versioning and publication in the intranet or Internet, and ultimately archiving.

Globally operating companies have to rely on a scalable distributed platform that caters to the many different capabilities of their employees and the demands of their target groups for intranet and Internet solutions. Livelink WCM Server enables companies to create, publish, and manage the entire spectrum of business-relevant content, and thereby ensures substantial optimization of company-wide business processes.

The main features and advantages of Livelink WCM Server are described briefly below.

Easy Content Editing

Livelink WCM Server offers several ways to edit website content:

- the Content client
- InSite Editing for modifying objects directly in the website

Content client

The Content client offers editors, graphics specialists, or quality assurance employees an intuitive user interface for editing website content. Any desired applications can be used for editing content, which means that authors can continue using their familiar tools and concentrate on their specific subject areas. The Content client is a website in its own right, and is based entirely on the WCM Java API.

The elements of the website are shown in a clearly arranged tree structure. An integrated HTML editor with WYSIWYG view allows you to edit HTML documents even without separate applications.

The Content client allows authors to edit website content no matter where they may be – access to the Content server, on which a website is located, is possible via LAN, WAN, or the Internet. Thanks to its extensive access control functions and communication encryption,
Livelink WCM Server guarantees protection for sensitive data.

InSite Editing

InSite Editing makes it possible to change or add content directly in your website. A simple click with the mouse during surfing in the Edit or QA view and – according to the WCM rights – context menus with the available edit functions are displayed. This makes it considerably easier to edit content.

Convenient Administration

The Admin client is provided for the configuration and administration of the content management system.

The Admin client serves as a single administration interface for all components of Livelink WCM Server. The components of a complex, freely scalable content management system based on Livelink WCM Server are configured and managed by means of a graphical user interface. Extensive system administration functions assist you in monitoring actions and solving problems.

Scalable Company-Wide Solution

Livelink WCM Server has a scalable server architecture. Websites are managed by a master Content server and can also be made available on any desired number of proxy Content servers. This makes Livelink WCM Server ideally suited to globally distributed, company-wide solutions and firewall architectures. As a Java implementation, Livelink WCM Server is platform-independent, thus supporting mixed environments.

The managed content is stored in a relational database management system (RDBMS) – Livelink WCM Server offers JDBC-based support for various RDBMS, for example Oracle. You can have central data storage facilities for the entire company or distributed data storage for different servers. The system architecture of Livelink WCM Server guarantees consistency of all content at all times, even with distributed data storage.

Livelink WCM Server is completely integrated in the Livelink product family. Thanks to its uncompromising support for open standards, such as Java and XML, and its powerful interfaces, the product also offers the option of integrating existing corporate solutions, such as application servers, commercial applications, or LDAP directory servers.

Reduced Costs Thanks to Reusability

Livelink WCM Server optimizes the cost of providing and maintaining a company-wide intranet or Internet solution.

Strict template-based separation of content and layout ensures compliance with company-wide corporate design rules and also reduces the effort required to create and update content. Both content and templates can be reused multiple times.

You can use Content Assembly, for example, to create assembled objects which consist of several fragments. The individual fragments can be used in multiple objects.

Up-to-Date Content

Up-to-date information is the key to customers' purchase decisions, and thus an essential requirement for enterprise portals. To ensure that website content is up-to-date, Livelink WCM Server offers a number of functions:

- content management during the entire life cycle and throughout all phases of the workflow
- support of time-controlled publication
- placeholders for object expiration dates
- full versioning of content
- integrated reference check to avoid “dead links” or graphics that cannot be displayed

Safety Through Risk Management

Critical business data used company-wide is protected by a variety of security mechanisms. For this purpose, Livelink WCM Server offers:

- comprehensive and flexible access control on the basis of users, groups, and roles for regulating access to website content, depending on section and object status
- configurable encryption of communication between servers and between clients and servers
- transaction security
- support of system architectures with firewalls
- use of security features of application servers and database systems

About this Manual

This manual describes the components and functions of the WCM system from the point of view of the system administrator. As the administrator of a WCM system, you should have a sound knowledge of the following fields:

- installation and configuration of a web server (HTTP server and JSP engine) or an application server
- standard methods of system administration, e.g. configuring and editing user administration systems, directory trees, and files
- administration of relational database management systems, such as Oracle
- administration of LDAP directory servers (optional)

In addition to this Administrator Manual, the following sources provide information:

- Livelink WCM Server Installation Manual: This document describes how to install the WCM system and configure web servers and application servers.
- Content Client User Manual: This manual provides detailed instructions on all tasks involved in editorial work on WCM-managed websites.
- Livelink Integration Manual: This document explains how to integrate your WCM system with a Livelink system.
- WCM Java API Programmer's Manual: This document contains information on interfaces, classes, and methods of the Java programming interface (WCM Java API), which enables you to use the functionality of the WCM servers via external programs.
- Portal Manager API Programmer's Manual: This manual contains detailed information on developing dynamic and personalized websites on the basis of the Portal Manager API.
- Online help – Livelink WCM Server offers an integrated online help that can be called at any time when working with the Admin client.

The contents of this manual are organized as follows:

- Chapter 2 “Concepts” explains the basic technical concepts of Livelink WCM Server.
- Chapter 3 “Working in the Admin Client” explains the general structure of the Admin client and constantly recurring workflows, such as creating assignments.
- Chapter 4 “User Administration” describes the user administration functions.
- Chapter 5 “Managing Pools and Connection Types” explains the configuration and administration of pools and connection types.
- Chapter 6 “Managing Servers” explains the configuration of WCM servers.
- Chapter 7 “Managing Websites” describes how to create and manage websites and associated elements, such as object types or object categories.
- Chapter 8 “Managing Deployment Systems” outlines the creation and administration of deployment systems.
- Chapter 9 “Managing Agents and Utilities” describes how to integrate and use agents and how to use utilities.
- Chapter 10 “System Administration” explains system administration functions, such as setting run levels of servers and websites, or report and tracing functions.
- Chapter 11 “System Overview” describes the function of the system overview, which offers you a clear summary of the structure and components of your WCM system.

Typographic Conventions

The following conventions are used in the text to draw attention to program elements, etc.:

Element	Font or symbol	Examples
Program interface such as menu commands, windows, dialog boxes, field and button names	*Menu → Entry*	*File → Create*
Paths to directories, file and directory names	**Drive:\Directory\File name**	**D:\WCM\ admin.bat**

Quotations from program code or configuration files	`Code quotations`	`<head>`
		`<title>heading </title>`
		`</head>`

Variables, i.e. placeholders for specific elements	{variable}	{WCM installation directory}

Important **information** and **warnings** are enclosed in gray boxes. Make sure to read such information to avoid losing data or making errors when using and managing WCM systems.

CHAPTER 2

Concepts

This chapter is intended to give you a basic understanding of the architecture of a web content management system (WCM system for short) and of the way Livelink WCM Server works. This knowledge is important when installing, configuring, and administering the system.

Basic Components of a WCM System

Livelink WCM Server is fully implemented in Java as a client/server solution. The data in the website(s) that you manage with
Livelink WCM Server is made available and managed by means of several servers. These are stand-alone server processes that can be started independently of each other. Taken together, all the WCM servers installed in a company make up a WCM system.

> **Note:** A WCM server is not a separate host computer; it is a server process. There can be several WCM servers installed on a single host.

One or more *websites* can be managed in a WCM system. A website can be published for Internet, intranet, or extranet access. The website objects that you manage with Livelink WCM Server (HTML pages, images, JSP scripts, etc.) are referred to as WCM objects. The WCM objects are stored in a relational database, such as Oracle or MS SQL Server.

In Livelink WCM Server, the objects of the website pass through fixed stages: editing, quality assurance, and publication for productive operation. This process is called *staging* and applies to all objects managed with Livelink WCM Server. Depending on the stage, there are different views of the WCM objects. For example, there may be changes to an object that have not yet been submitted to QA, and of course, not yet released for productive operation.

The different views of the WCM objects are provided by the so-called *deployment systems*. They generate files, e.g. HTML pages or JSP files, from the WCM objects that are stored in the database. The generated files can be displayed in a web browser. The generated files are distributed to the file system of the Content servers on which the website is accessible. From there, they become visible for the user via an HTTP server. Editing and quality assurance are carried out by means of the Content client. Subsequently, the objects are released for productive operation and are thus made visible to all users.

The following figure illustrates the structure of a WCM system and the associated environment.

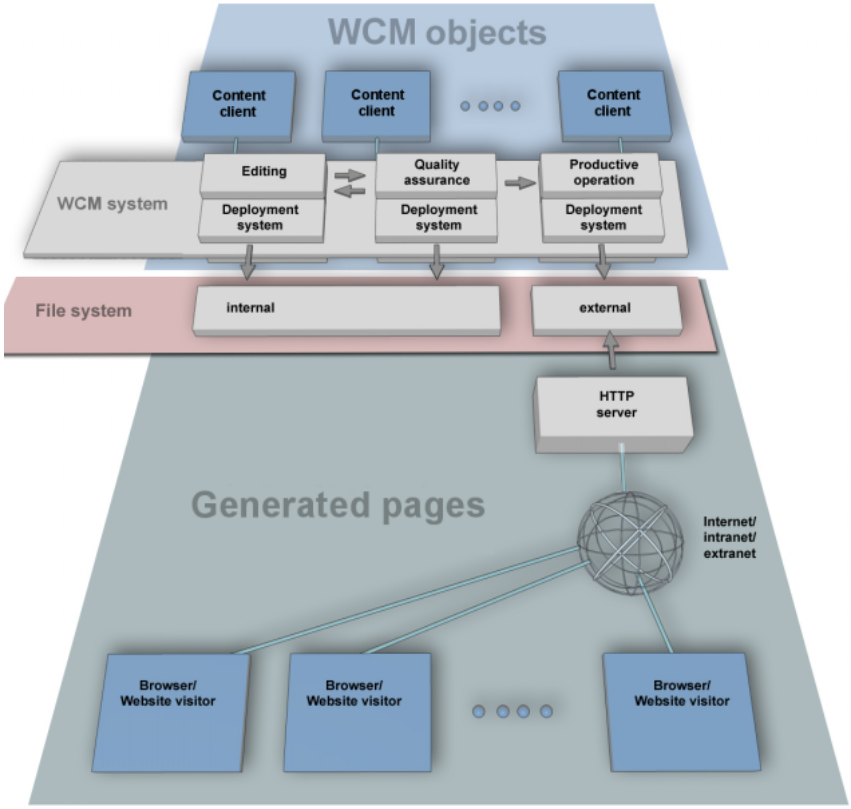


Fig. 1 – Simplified WCM system and its environment

The following sections describe the basic components of a WCM system. These include:

- the staging and workflow of Livelink WCM Server
- the WCM servers
- the deployment systems
- how user and website data is stored
- communication between the individual components of the WCM system
- available programming interfaces

The Staging and Workflow of Livelink WCM Server

All objects of the websites that you manage with Livelink WCM Server pass through fixed stages: editing, quality assurance, and publication for productive operation. Editing and quality assurance of the objects is carried out in the Content client. After publication, the objects can be accessed via a browser. Passing through these stages is called *staging*.

In addition to the staging, you can assign a *workflow* to certain objects, e.g. for successive editing by several editors or for multi-stage quality assurance.

Staging

According to the current processing stage of a WCM object, there are different views of the object: Edit, QA, and Production view.

Edit view

In the Edit view, WCM objects, such as HTML pages, are added and edited by editors and graphics specialists. These users need corresponding access rights for the objects. The Edit view shows the current processing status of the WCM objects. The respective HTML pages are, by default, generated on the basis of the released templates.

After they have been edited, the objects are submitted to Quality Assurance. This makes new objects or changes to existing objects also visible in the QA view.

QA view

The QA view shows the WCM objects with all changes that have been submitted to Quality Assurance. Quality Assurance staff can check the changes with regard to content and formal aspects. On the basis of this check, they decide whether an object is to be sent back for correction or to be released. For release, the respective access right is required. After the release, the objects become visible in the Production view. Thus, the current version becomes available in the published website.

Production view

The Production view makes the released pages of a website available to the website visitors. By means of an HTTP server, these pages can be accessed via the Internet or intranet.

The following figure illustrates the different stages and the actions that realize the transitions between the stages.

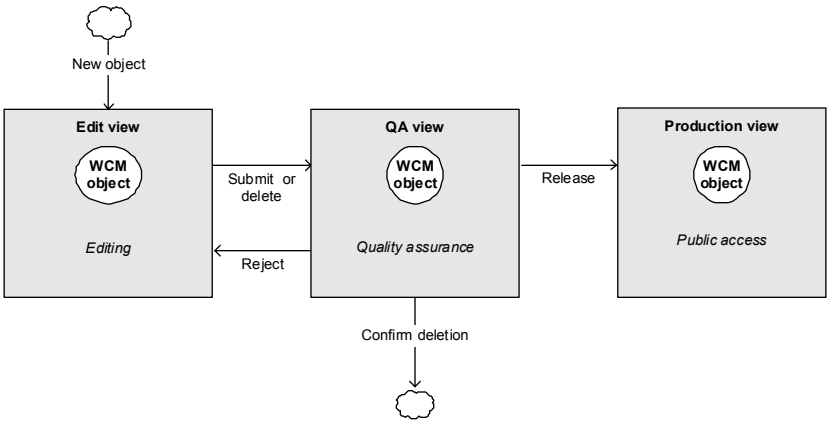


Fig. 2 – The staging of Livelink WCM Server

Workflow

To extend the predefined editing and publication stages of WCM objects by custom workflow steps, you can assign a workflow to a WCM object. Depending on the processes in your company, this workflow may contain several Edit and QA steps.

When the workflow is created in the Content client, certain users are assigned to the workflow steps. Only these users are allowed to edit the respective objects within these workflow steps. Of course, the users also need sufficient object rights.

After editing the WCM object, the user simply selects one of the predefined workflow steps in order to forward the object to the next user or to return it to the previous workflow step. The “normal” staging actions (submit, reject, release, etc.) are not available. The necessary staging transitions are automatically performed in the background.

The following diagram illustrates an example workflow.

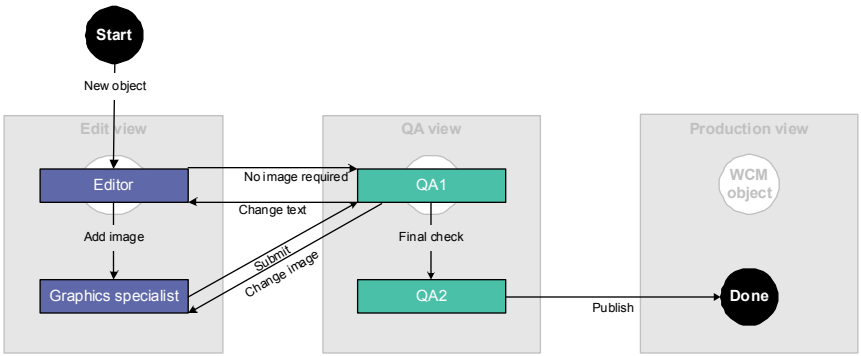


Fig. 3 – Example workflow in Livelink WCM Server

Note: For detailed information on working with staging and workflow, refer to the Content Client User Manual.

The Server Concept of Livelink WCM Server

The servers that make up a WCM system are divided into different server categories and server types.

The Server Types

According to the tasks of the servers, there are two server types:

- Content servers for managing website data
- Administration servers for managing user, configuration, and system data of the WCM system

Basically, every Content server is able to provide all views of the data of the managed websites – Edit, QA, and Production. The available views may be limited by the fact that the Content server only receives the data of certain views. This is determined by the *routing* between the Content servers. This way, you can limit the data volume transferred between the different Content servers. For example, a proxy Content server outside the company firewall should only have the Production view of the website data because WCM objects are not edited there. For general information on routing, please refer to section “Routing Between the Servers” on page 47.

Depending on the available view, different types of deployment systems (Edit, QA, and Production) can be installed on a Content server, see “The Deployment System Types” on page 37.

Important! For editing the WCM objects by means of the Content client or Content client (Classic) of Livelink WCM Server, the respective Content server must have all three data storage views and run in the context of a JSP engine or as a web application in an application server.

The Server Categories

The servers are divided into two main categories: **master** and **proxy**. In every WCM system, there is one master Administration server and one or several master Content servers.

The **master Administration server** handles user administration and is responsible for configuration, system administration, and license management. The Administration server can be accessed using the Admin client of the WCM system.

The **master Content server** manages one or more websites. Each website is assigned to exactly one master Content server. Changes to the content and status of WCM objects can only be made on a master Content server. The master Content server always has all data storage views (Edit, QA, and Production).

In addition to the master Content server, you can set up **proxy Content servers** in your WCM system, which also provide access – by way of deployment systems – to the website data. Unlike a master Content server, however, proxy Content servers merely have read-only access to the content. If website data is to be edited using a proxy Content server, the proxy Content server consults the master Content server, which locks the object from further write accesses and, once editing is complete, stores the changed objects in the data storage. The master Content server then informs all proxy Content servers connected to the website that the WCM object has changed. This ensures that your website content remains consistent.

The following diagram illustrates the tasks of the master and proxy Content servers in a WCM system.

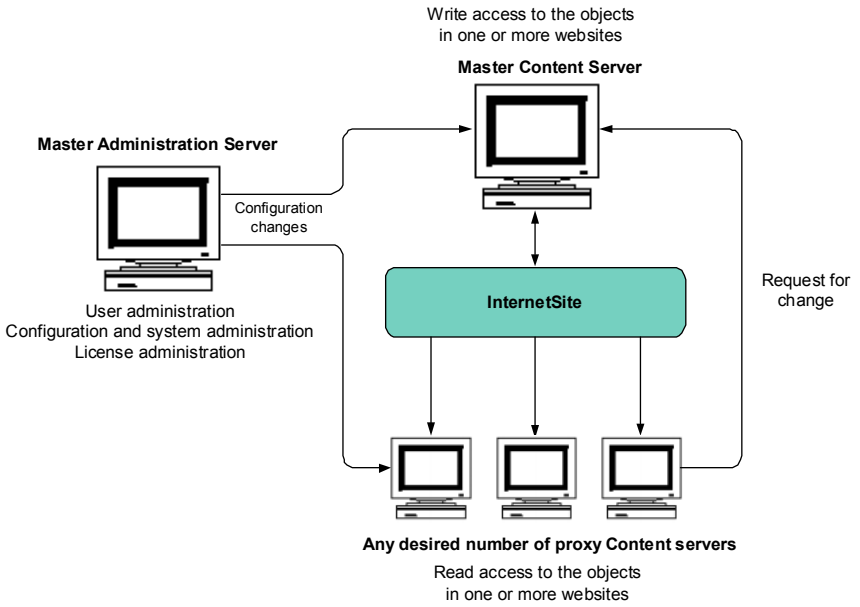


Fig. 4 – WCM system consisting of master and proxy Content servers

Using proxy Content servers has several advantages:

- Different views of a website (Edit, QA, and Production) can be distributed to different proxy Content servers.
- The workload in the WCM system can be distributed among several Content servers. The only tasks left to the master Content server are to change the data and to notify the connected Content servers of the changes. This notification is bound to the website. If you manage a number of websites in your WCM system, then for any change made to a website, only the relevant proxy Content servers for that website will be notified.
- Since changes to website content can only be made on the master server, consistency of the content is guaranteed.

- Data transfer between the Content servers is optimized by Livelink WCM Server. This reduces the data volume to be transferred, allowing you to connect systems that only have access to a slow communication connection. Also, you can adapt the communication between the servers to suit the situation in your network. See also “Communication Between the Components of a WCM System” on page 46.
- You can set up distributed systems with proxy Content servers outside a firewall.

As with the Content servers, it is also possible to set up **proxy Administration servers**. This is, for example, required if you use a highly distributed WCM system with several proxy Content servers. Instead of establishing a connection to the master Admin server, the servers can contact a proxy Admin server to request information on configuration, user administration, or licenses. A proxy Admin server is also required for setting up a WCM system with proxy Content servers outside a firewall, see “Distributed System with Firewall” on page 57.

Content and Administration servers are set up using the WCM installation program. For detailed information, refer to the Livelink WCM Server Installation Manual. Servers are managed in the *Configuration* view of the Admin client, see chapter 6 “Managing Servers”.

Deployment

Deployment, in a more general sense, describes the distribution of data, programs, operations, etc. for any further processing needs. In the context of Livelink WCM Server, deployment is the task of making WCM objects available in the form of files in the file system of the Content servers. From there, they become visible for the user via an HTTP server. Provided there is also a JSP engine available on the HTTP server machines, the objects of the website can be edited with the Content client.

The deployment for the WCM system has two main tasks:

- **generating pages for the WCM objects:** Deployment systems can be installed on every Content server. A specific type of deployment system (Edit, QA, or Production) is responsible for each view of the website data. The deployment systems generate pages for the WCM objects and distribute these files to the file system of the corresponding Content servers. In the generation process, they have to perform such important functions as determining the storage location for the generated page, replacing references, and generating hyperlinks. Depending on their category, deployment systems also fulfill tasks such as combining content and template, replacing WCM tags, statification, and preparing the pages for the functionality of the Content client.

  > **Note:** For detailed information on page generation, refer to the Content Client User Manual.

- **notification in case of changes:** The deployment inform the Content servers about changes to WCM objects, creation of websites, etc.

A deployment system is characterized by various criteria:

- the Content server on which it is installed
- the website for which it generates pages
- the type, corresponding to the staging concept of Livelink WCM Server (Edit, QA, and Production)
- the category, i.e. the way deployment jobs are processed

Deployment systems are set up when creating a website and can also be added to the WCM system at a later stage. See also chapters 7 “Managing Websites” and 8 “Managing Deployment Systems”.

The Deployment System Types

In accordance with the staging concept of Livelink WCM Server, the deployment systems are divided into three types: Edit, QA, and Production. An Edit deployment system generates the Edit view of the website data; a QA deployment system the QA view, etc.

Depending on the data storage view, only certain types of deployment systems can be installed on a Content server. The data storage view available on a Content server is determined by the routing settings of the website (see “Routing Between the Servers” on page 47). On a Content server with Edit view, you can set up Edit, QA, and Production deployment systems. By doing this, you can provide access to all three views of the WCM objects of your website on this server. On a Content server with QA view, QA and Production deployment systems can be installed. On Content servers with Production view, only Production deployment systems are possible.

The following table illustrates the relationship between data storage views and deployment systems.

Table 1 – Data storage views and possible deployment systems (DS)

Available data storage view	Edit DS	QA DS	Production DS
Edit	✓	✓	✓
QA		✓	✓
Production			✓

Based on this technology, it is possible to set up a flexible and scalable WCM system. You have the option of installing all data storage views and the respective deployment systems on a single host, or you can set up a distributed system with several Content servers and install different types of deployment systems, depending on the routing.

If you use Livelink WCM Server to manage different websites, you can set up the deployment systems for these websites on one Content server, e.g. the QA and Production deployment systems for the website “CompanyIntranet“ and the QA deployment system for the website “InternetSite”. Thus, three deployment systems are available on this proxy Content server. A system of this kind is described in section “Distributed System with Two Websites” on page 62.

The Deployment System Categories

The category of a deployment system determines the way in which deployment jobs are processed. The following categories exist:

- standard deployment system (see the following section)
- dynamic deployment system (see section “Dynamic deployment system” on page 40)
- search engine deployment system (see “Search engine deployment system” on page 42)

- WebDAV deployment system (see “WebDAV deployment system” on page 42)
- InSite Editing deployment system (see “InSite Editing deployment system” on page 43)

Standard deployment system

Standard deployment systems automatically generate a new page every time a WCM object is changed (static deployment). The generated pages are stored in the file system. For this reason, access to the pages of standard deployment systems is usually fast, as the HTTP server can read the objects directly from the file system.

However, it is possible that when an edited WCM object is accessed, the generated page has not yet been updated by the deployment system, with the result that the “old” version is displayed in the Content client or via the HTTP server. This may occur if there are large numbers of deployment jobs to be processed.

This deployment system category is well suited when many users access the generated pages at the same time, but only a few changes are made to the objects. This applies, for example, to the Production view of the website data.

Standard deployment systems can store the generated pages in a hierarchical or a flat file structure. In a hierarchical file structure, each topic of the website corresponds to a directory. A flat file structure does not reflect the topic structure of the website. This considerably reduces deployment load, e.g. when copying and moving objects.

Dynamic deployment system

Dynamic deployment systems do not generate the pages statically when the WCM object changes, but dynamically when the page is requested by the HTTP server. If a changed object is accessed, the deployment system generates the corresponding page. Although this makes access slower, the current status of the object is always displayed as soon as the deployment system has noticed that the generated page must be changed.

Dynamic page generation is especially advantageous if many changes are made to the WCM objects, e.g. for the Edit view. When using the import functions or when cutting, copying, and pasting objects, the advantage becomes especially apparent.

Simultaneous access to the generated pages by many users may result in a high workload for the host computer because the respective pages have to be generated for each access to changed WCM objects. Thus, a dynamic deployment system is not very recommendable for the Production view, which is accessed by many users simultaneously.

The deployment metadata (URLs, directories, etc.) are automatically updated in the database when the WCM objects are changed, only page generation is performed on demand. This reduces the workload on the host computer, because page generation and the resulting file access do not have to be performed every time a WCM object changes.

Dynamic deployment systems can generate pages for different versions of the WCM objects:

- for the different data storage views Edit, QA, and Production
- for different template versions (released template or current template in the Edit view)
- for the object version at a certain point in time
- for the view of a specific user

The current version of the objects in the Production view is displayed, including all changes the respective user has made. Additionally, all changes that other users made before the object was edited by the selected user are displayed.

In the Configuration dialog box of the Content client, you determine which of these options to apply to the dynamic deployment. This way, the users can control individually how they want to display the generated pages in the Content client.

By default, the generated pages are stored in the local file system of the Content server. As the dynamic deployment system can generate different views of the WCM objects (see above), the page is only stored in the file system if the settings for generating the page correspond to the default settings of the deployment system and if the released template is used. If this is not the case, the page is generated temporarily. This means that pages which were generated based on individual user settings are not stored in the file system. The pages stored in the file system are used as a cache – when one of these pages is accessed the next time, it can be loaded directly from the cache if the WCM object has not been changed in the meantime. This makes access to these objects faster. Access to temporarily created pages is, however, slower because the page must always be generated.

Dynamic deployment systems store the generated pages in a flat file structure. The topic structure of the website(s) is not reflected in the directory structure. This considerably reduces deployment load, e.g. when copying and moving objects.

For the dynamic deployment, a servlet is used. For this reason, the respective Content server must run in the context of a JSP engine or as a web application in an application server. For information on the configuration of JSP engines and application servers, refer to the Livelink WCM Server Installation Manual.

Search engine deployment system

You can use this deployment system category to prepare your website data for being processed by a search engine. A search engine deployment system works on a static basis and only processes selected object types. Graphics, for example, are by default not included in this deployment, as they cannot be used for indexing and processing search requests.

Moreover, you can define metadata that are to be included in the indexing process of the search engine. Thus, it is also possible to find metadata that are not included in the content of an object.

Only the content is processed in page generation – any templates used are not included, and references are not processed. The WCM tags are, however, replaced. The generated files are stored in a flat file structure.

WebDAV deployment system

The WebDAV (Web-based Distributed Authoring and Versioning) protocol supports Internet and group-based working on the basis of standard Internet technologies. Thanks to WebDAV, users do not need a special client for creating WCM objects, jointly editing them, and managing them by means of WevDAV-capable tools.

A WebDAV deployment system is required for using WebDAV. This is a dynamic deployment system that does not process the pages statically when the WCM object is changed, but dynamically updates them when the page is requested by a client. For accessing objects with WebDAV-capable clients, a servlet is used. Thus, WebDAV deployment systems can only be installed on Content servers running in the context of a JSP engine or as a web application in an application server.

A WebDAV deployment system supplies the Edit view of the WCM objects. For this reason, the routing of the website must be configured in such a way that the respective Content server has the Edit view (see “Routing Between the Servers” on page 47).

The generated files are stored in a hierarchical file structure. Each topic corresponds to a directory on the Content server's host computer. A separate file represents the content of the topic.

Only the content is processed in page generation – any templates used are not included, and WCM tags are not replaced.

InSite Editing deployment system

This deployment system category provides the basis for editing and adding content directly in your website – without the Content client. With the proper WCM rights, you can display context menus with the available edit functions in the Edit or QA view. This makes it considerably easier to edit content.

InSite Editing deployment systems are dynamic deployment systems (see above).

Storing the Website Data

Each website object consists of a series of metadata that are used to create, manage, and classify objects. These include the content of WCM objects such as texts, graphics, or JSP scripts. The metadata also include attributes, properties, and access control information. The object metadata are stored in an external relational database, such as Oracle. The stored data is used by the deployment systems to generate the physical representations of the objects, e.g. HTML files.

> **Note:** For information on integrating Livelink WCM Server with an RDBMS, refer to the Livelink WCM Server Installation Manual.

All Content servers belonging to a WCM system can access a common data storage. This keeps the communication traffic between servers to a minimum because the metadata and the object content only have to be sent to the proxy Content servers if an object is requested by a proxy Content server. When a WCM object is changed, the master Content server informs all connected proxy Content servers about the change. The relevant object is removed from memory on the proxy Content servers and is reloaded from the common data storage the next time it is requested.

If your company's websites are maintained and managed in a distributed infrastructure (e.g. with offices in Germany and in the US), you also have the option of equipping the proxy Content servers with their own data storage. The main task of a distributed data storage system is to reduce the transfer of data between servers. If a proxy Content server requests a WCM object, it is read from the local database. However, as in the case of the central data storage, the changes are made on the master Content server. The master Content server then notifies all relevant proxy Content servers about the changes and transfers the changed content and meta-data to the remote databases. This ensures that the WCM objects are identical in all databases. A scenario of this kind is described in section "Distributed System with Separate Data Storage for Proxy Content Servers" on page 60.

All previously released versions of an object and any versions generated since the last release are stored in the database of the master Content server. The archived versions can be restored at any time. Via the Admin client, you can control how many versions of the WCM objects are archived in the database. Older object versions are restored via the Content client.

Storing the User Data

There are three possibilities to store the users, groups, and roles (the so-called *principals*) of the WCM system:

- using a relational database (as for storing website data)
- using a Livelink user administration
- using an LDAP directory service

You must determine which of these possibilities you want to use before installing Livelink WCM Server. For this decision, consider the following:

- Does your company already have a central user administration – e.g. on the basis of an LDAP directory service – that you want Livelink WCM Server to access?
- What is the architecture of the planned WCM system? For distributed WCM systems in particular, we recommend the use of an LDAP directory service.
- Is a Livelink system available whose user administration can be accessed?

For detailed information on the preparations required for using a database or an LDAP directory service, refer to the Livelink WCM Server Installation Manual. For information on using a Livelink user administration, refer to the Livelink Integration Manual for the WCM system.

If you use an LDAP or Livelink server for managing users, the user information is not stored in the database of the WCM system, but only in the LDAP or Livelink server. This ensures company-wide consistency of this data. When a user logs in, the master Admin server of the WCM system contacts the LDAP or Livelink server, which then performs the user's authentication.

When you set up a distributed WCM system with one or more proxy Admin servers, it is possible that these servers do not access the master user administration, but a second database, a second LDAP directory service, or a second Livelink server. This speeds up access to the user data for all proxy Content servers managed by the proxy Admin server in a distributed WCM system. An example of such a system is described in section “Distributed System with Firewall” on page 57.

You can manage the users, groups, and roles via the Admin client no matter where the users of the WCM system are stored. For detailed information, refer to chapter 4 “User Administration”. In the case of an LDAP directory service or a Livelink user administration, it is also possible to use the familiar administration tool for the respective product.

Communication Between the Components of a WCM System

The components of a WCM system communicate with each other via a LAN or WAN. Within a WCM system and beyond, numerous communication connections are required, e.g. for the following purposes:

- Master Content servers inform connected proxy Content servers about changes to website data.
- In the context of staging and workflow, e-mail notifications are sent. For this purpose, the servers require a connection to an SMTP server.
- Each Content server must be able to connect to an Admin server in order to load configuration and license information.

Note: When planning your WCM system, make sure that the required routing channels are available. For information on the structure of a WCM system, refer to section “Scenarios for Setting up a WCM System” starting on page 55.

Communication between the components of a WCM system is influenced by the following factors:

- routing between the servers
- the protocol used
- the settings of the pools in which the connections are managed

Due to the flexible system architecture of Livelink WCM Server, a WCM system can be distributed over a LAN or WAN. It might be necessary to exactly control the communication between the components of the WCM system, e.g. for integrating firewalls. The following sections provide basic information on communication.

Routing Between the Servers

Changes to the WCM objects are always saved by the master Content server. This informs all connected proxy Content servers about the changes and sends them the changed data.

You can determine which Content server is to be informed by which other Content server about changes to this website and which data storage view is transferred. In certain cases, it may be advisable, for example, that the receiving Content server does not get the Edit view of the data (with the largest data volume possible), but only the Production view (with the smallest data volume possible). This applies, for example, if the proxy Content server is located outside a firewall and publishes the Production view of the website.

In distributed systems with connections of different speeds between the Content servers, it may be advantageous to change the standard routing. Please note that a sending server can only forward the data view that it receives or a view with a smaller data volume.

You can determine the routing between the Content servers in the *Configuration* view of the Admin client:

- during user-defined creation of a website, see “Creating a Website with the Option User-defined” on page 218
- during assignment of proxy Content servers to a website, see sections “Websites Assigned to Servers” on page 177 and “Proxy Content Servers Assigned to a Website” on page 228

Communication Protocols

All network connections used in the WCM system are based on TCP/IP or UDP/IP. For communication between the clients of the WCM system and the servers, as well as for communication between the servers, either the proprietary protocol VIPP or the HTTP protocol can be used. For both protocols, different ports are configured.

The following diagram illustrates the communication on the basis of a layer model.

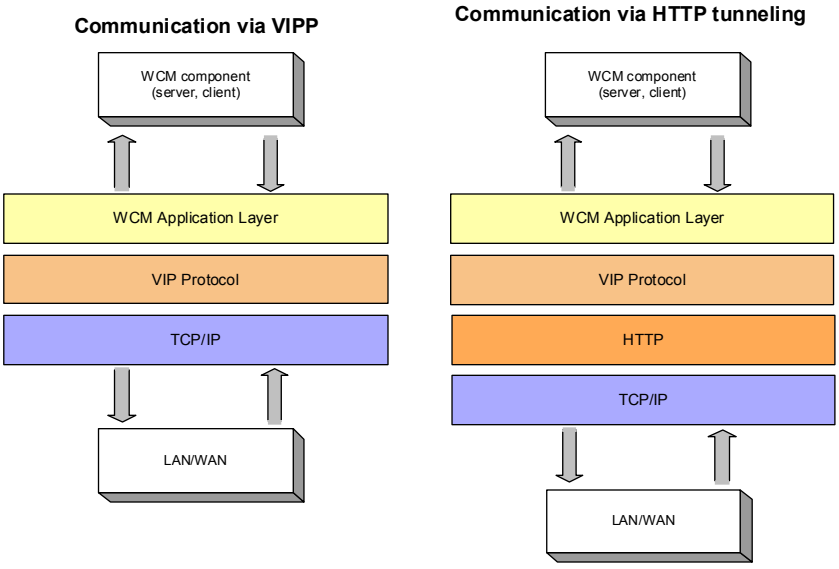


Fig. 5 – Communication via VIPP and HTTP tunneling

To improve security, it is possible to use SSL (Secure Socket Layer) for both VIPP and HTTP tunneling. This protects communication between the components of the WCM system from eavesdropping and falsification.

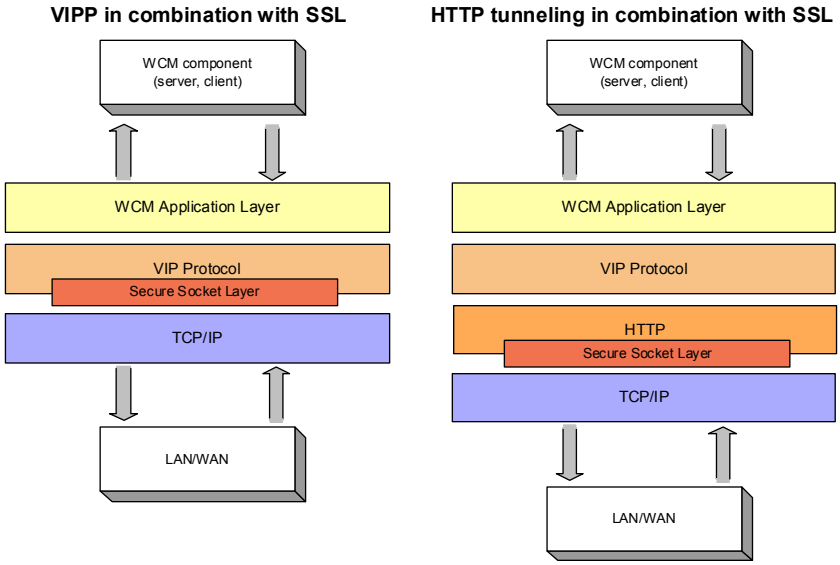


Fig. 6 – Use of SSL for VIPP and HTTP tunneling

For the connection to third-party systems, a number of different protocols are used:

- connections to the RDBMS: proprietary protocols of the JDBC drivers
- connections to the LDAP directory service: LDAP (version 3)
- connections to Livelink: proprietary Livelink protocol
- connections to the mail server: SMTP
- connections to the HTTP servers: HTTP protocol (version 1.1)

Pools

In a WCM system, different connections are required for the following purposes:

- data transmission between Livelink WCM Server and the RDBMS
- communication between the servers and between clients and servers
- communication with an LDAP directory service
- communication with a Livelink system
- connection to third-party systems

Usually, it is quite time-consuming to establish a connection. This can be particularly inconvenient if data is sent frequently (e.g. concerning notification about changes to content or configuration), but the data volume transferred is low. For this reason, the connections for a WCM system are managed in **pools**. This gives you the opportunity to define – depending on your system's requirements – how many connections you want to be established immediately when a server starts up and how many you want to kept open all the time the server is running.

If a connection is required for data transmission between the components of a WCM system, it is taken from the respective pool. When the transmission is complete, the connection is returned to the pool.

For each connection purpose, e.g. the connection to an RDBMS, there is a special **connection type** provided with all parameters required. During installation, the default connection types are created automatically:

- connection type "JDBC" for connections to relational databases
- connection type "LDAP" for connections to LDAP directory services
- connection type "Livelink" for connections to Livelink systems
- connection type "WCM" for connections between the servers

In addition to the default connection types, you can configure custom connection types, e.g. for integrating third-party systems, and set up corresponding pools.

On the basis of the default connection types, the installation program automatically adds the required pools for the connections of the WCM system. Pools and connection types are managed in the *Configuration* view of the Admin client, see chapter 5 “Managing Pools and Connection Types”.

In order to adapt the communication between the components of the WCM system to the situation in your LAN or WAN, you can modify the settings of the pools that were set up during installation. Moreover, it is possible to add pools on the basis of the default connection types or custom connection types. This way, you can integrate several databases, LDAP servers, or Livelink systems in the WCM system and realize an integration with third-party systems. For detailed information on adding pools, refer to section “Adding a Pool” on page 162.

Notes:

Not all connections of the WCM system are managed in pools, e.g. the connections to Search servers, HTTP servers, and SMTP servers.

Starting a Content server is a special case. At this time, the server does not know the pool configuration yet. For this reason, a so-called *individual WCM connection* is used for the connection to the responsible Administration server. For information on the configuration of this individual WCM connection, please contact the Technical Support of Gauss Interprise AG.

Optimizing communication between the servers

During the installation of the servers, pools of type “WCM” are automatically created. These pools have the name of the respective server and provide the parameters for establishing a connection to this server. By default, all other servers use these parameters to contact the respective server.

In a distributed WCM system with slow and fast connections and firewalls between the components, it is often not possible for all servers to use the same communication parameters. A proxy Content server might, for example, be separated from the master Content server of the website by a firewall. In this case, it might be necessary to use the protocol HTTP for the connections from the proxy Content server to the master Content server.

To optimize the integration of the servers in a distributed network environment, you can set up special pools of type “WCM” for the connection between two servers. These pools provide the parameters required for establishing connections in one direction: in this example, in the direction proxy Content server → master Content server.

The extended settings of WCM pools offer you detailed configuration options for adapting communication to the situation in your corporate network. You can define special ports and IP addresses for establishing connections, modify buffer sizes and timeouts for slow connections, or configure the use of a tunnel or an HTTP proxy. For detailed information on the individual parameters, refer to the online help of the Admin client.

Programming Interfaces

Livelink WCM Server offers flexible programming interfaces for using the core functionality of Livelink WCM Server via external programs. Different interfaces are available:

- WCM Java API
- Portal Manager API
- WCM WebServices

In the following, the programming interfaces are briefly described.

WCM Java API

The WCM Java API offers a defined interface for integrating external Java programs in the WCM system. This may be so-called server agents that are executed within a server, or external programs that access a server from a remote computer.

Once an external program has registered itself, it is activated in defined circumstances:

- when an event occurs (e.g. adding, deleting, or moving a WCM object)
- when a defined status in the sequence control is reached

Programs that use the WCM Java API must be implemented in Java. They have access to, among other things, staging operations, administration functions, and system administration information of Livelink WCM Server.

For information on integrating server agents, see section “Managing Server Agents” starting on page 282. Information on how to use the WCM Java API can be found in the WCM Java API Programmer's Manual.

Portal Manager API

The Portal Manager API is available if the respective Content server runs in the context of a JSP engine or as a web application in an application server.

The Portal Manager API enables you to create and manage dynamic content for your website, thus allowing you to develop enterprise portals. Furthermore, the Portal Manager API forms the basis for personalizing websites. You should consider it as a framework that helps you create web portals and web applications.

For detailed information on using the Portal Manager API, refer to the Portal Manager API Programmer's Manual.

WCM WebServices

Web Services are a technology for realizing distributed work over the Internet. They allow the communication between programs written in different programming languages and running on different platforms via the standardized protocol SOAP. Another great advantage of Web Services is the use of standard web formats and protocols: XML, HTTP, and TCP/IP.

WCM WebServices offers a WCM-specific API that can be used independently of the programming language. Similar to the WCM Java API, you can use Livelink WCM Server core functionality via this API. The following is offered, among other things:

- all object data types know in the WCM system
- accessing content and metadata of WCM objects
- availability of staging operations (check out, check in, submit, release, direct release, etc.)
- performing complex search requests

Quite a large number of programming languages are Web Services-capable. For example, ASP.NET, C#, and Visual Basic can be used.

For detailed information on using WCM WebServices, refer to the WCM WebServices Programmer's Manual.

Scenarios for Setting up a WCM System

Because of the flexible system architecture with master and proxy servers, there are numerous possibilities for setting up a WCM system. Since you can add further servers and deployment systems any time, Livelink WCM Server also enables you to expand an installed system if your company's requirements change.

The following section describes several scenarios to illustrate the basic approach.

Notes

- Each of the scenarios described below focuses on one aspect of setting up a WCM system (distribution on multiple proxy Content servers, integration of a firewall, separate data storage, etc.). A real WCM system will normally involve a combination of different aspects.
- The Portal Manager API is available on all Content servers running in the context of a JSP engine or as web applications in an application server. This is also required for using the Content client and the Content client (Classic).
- Due to the restrictive lock mechanism of MS SQL Server, we recommend that you set up separate databases for the master Content server and the proxy Content servers. This ensures that read access of the proxy Content servers is not blocked by actions that are performed on the master Content server.

Minimum System

The WCM system consists of a master Admin server and a master Content server. The master Content server is executed in the context of a JSP engine or as a web application in an application server.

The website “InternetSite” is created on the master Content server. The website objects are distributed to different directories via three deployment systems (Edit, QA, and Production). Thus, the complete staging is realized on the master Content server. In the figure, “DS” is the abbreviation for “deployment system”.

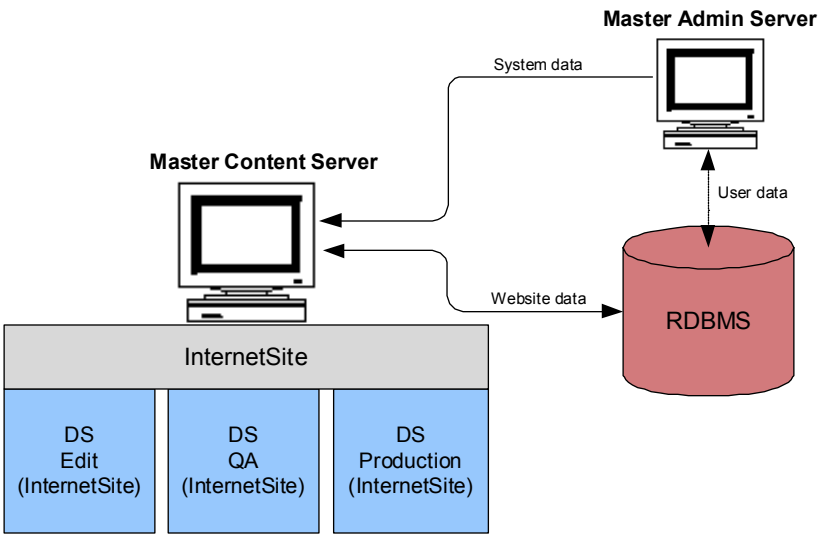


Fig. 7 – Structure of a minimum system

The master Admin server manages the system data, such as license information and server configuration, and sends this data to the master Content server. Since the user data can be stored in either a relational database, an LDAP system, or a Livelink system, the connection of the master Admin server to the RDBMS is optional.

The master Content server manages the website data. The WCM objects are stored in a relational database, which is available to the master Content server for read and write access.

A minimum system is installed by selecting the relevant option in the WCM installation program (see Livelink WCM Server Installation Manual). When creating a website in a minimum system with the Admin client, you are guided by the website wizard (see “Creating a Website with the Option Minimum or Minimum (dynamic)” on page 207).

Distributed System with Firewall

The WCM system consists of a master Admin server, a master Content server, and a proxy Content server behind the firewall, i.e. within the corporate network. The proxy Content server within the corporate network runs in the context of a JSP engine or as a web application in an application server. It is used for editing and quality assurance of the WCM objects by means of the Content client. For this reason, two deployment systems for the website “InternetSite” are installed on this server.

Outside the firewall (outside the company network), there is a proxy Content server, on which the Production view of the website is published, and a proxy Admin server. This proxy Admin server is needed by the proxy Content server for loading the server configuration on startup, logging in users to the WCM system, and checking the license. The proxy servers outside the firewall use a separate database.

All changes to WCM objects are made in the master data storage via the master Content server. Changed WCM objects and notifications of changes are sent by the master Content server to the proxy Content servers.

The master Admin server informs the proxy Admin server about configuration changes and transmits the changed configuration data. The proxy Admin server stores the configuration data in the form of XML files in the local file system. Changes to the configuration are not possible on the proxy Admin server; the configuration can only be viewed. All changes are made on the master Admin server. In this way, the configuration data on both Admin servers is always identical.

If the user administration information is stored in a relational database, all changes in the user data are only made via the master Admin server. Changed user data is not automatically sent from the master Admin server to the proxy Admin server. Synchronization of the user data in the two databases can be controlled by means of a script, for example. If you use an LDAP or Livelink server for user administration, a second LDAP or Livelink server can be installed outside the firewall. The WCM system does not automatically synchronize the two servers. Use the corresponding functions of the LDAP or Livelink system for this purpose.

In a distributed system with a firewall, communication between the servers through the firewall mostly takes place via HTTP, in our example, between master Admin and proxy Admin server and between master Content and proxy Content server. You can determine the parameters for communication through the firewall in the settings of the respective WCM pool.

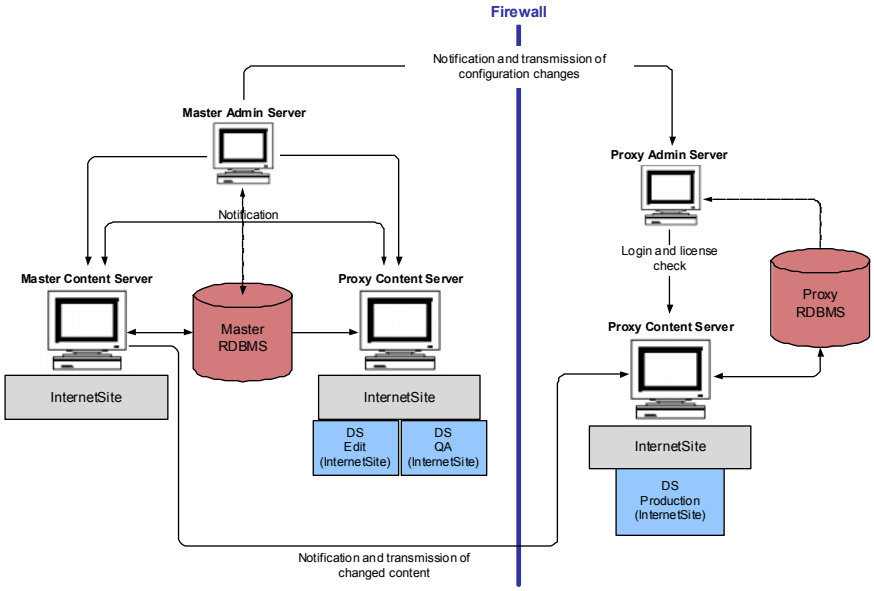


Fig. 8 – Distributed WCM system with firewall

In this example, the proxy Content outside the firewall is informed of changes by the master Content server. Since it is possible to configure the routing between the servers, depending on the requirements of your LAN or WAN, it would also be possible that the proxy Content server outside the company network is notified by the proxy Content server within the company network. The routing should be configured in such a way that the proxy Content server outside the company network only gets the Production view of the website data. This significantly reduces the data volume to be transferred. For information on the routing, refer to “Routing Between the Servers” on page 47.

A distributed system of this kind is created using of the option *User-defined installation* in the WCM installation program (see Livelink WCM Server Installation Manual). When creating a website with several proxy Content servers and separate databases, you can obtain assistance from the new-website wizard, see “Creating a Website with the Option User-defined” on page 218.

Distributed System with Separate Data Storage for Proxy Content Servers

The WCM system consists of a master Admin server and a master Content server. The website “InternetSite” is created in the WCM system. The system is distributed among three additional proxy Content servers. Two of these proxy Content servers run in the context of a JSP engine or as a web application in an application server. They are used for editing the WCM objects by means of the Content client. Thus, the respective Edit and QA deployment systems are installed on these two servers. The third proxy Content server is used for publishing the Production view of the website. On this server, a Production deployment system is installed.

The following procedure guarantees that the data in the master and proxy data storages are always identical:

1. If, for example, a WCM object is edited via a proxy Content server, the proxy Content server informs the master Content server that the object is being edited. The master Content server locks the object so that it cannot be edited by other servers at the same time.
2. On the proxy Content server, the object is loaded from the proxy data storage. It is edited in the Content client.

3. The proxy Content server receives the edited metadata and content and sends them to the master Content server. The master Content server checks whether the changes are permitted and then stores the changed data in the master data storage.
4. The deployment distributes the changed data to the proxy Content servers.
5. The data transferred from the master Content server is stored in the proxy data storage. Thereby, both databases are synchronized.

In the following diagram, the connections from the master Admin server to the other servers are not shown.

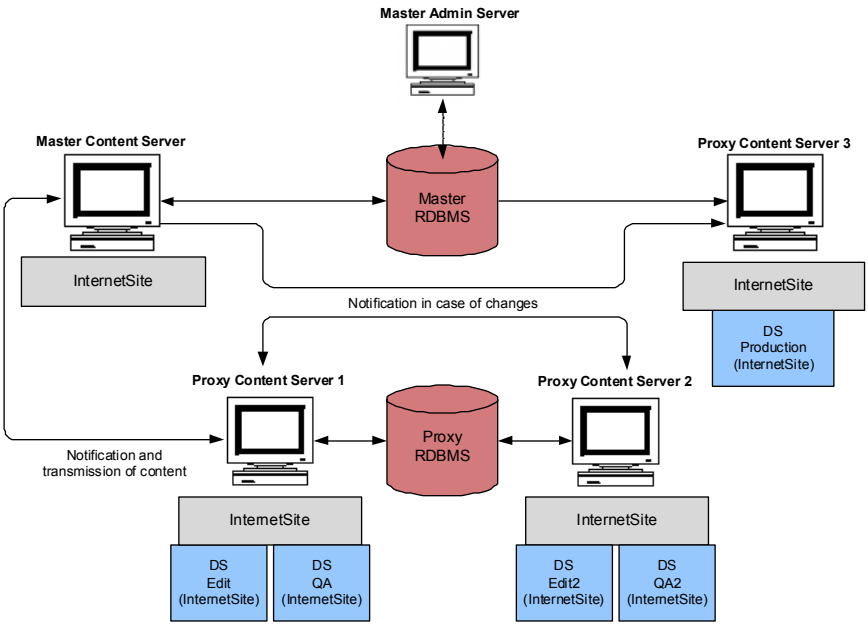


Fig. 9 – Distributed WCM system with separate databases

If a WCM object is changed, the master Content server informs the proxy Content servers 1 and 3. Proxy Content server 1 informs proxy Content server 2 about the changes. Deployment for the changed objects is carried out on all the notified servers, so that the corresponding pages are updated.

You can adjust the communication between the servers of your WCM system to best suit the requirements of your LAN or WAN, see “Communication Between the Components of a WCM System” on page 46.

A distributed system of this kind is created using of the option *User-defined installation* in the WCM installation program (see Livelink WCM Server Installation Manual). When creating a website with several proxy Content servers and separate databases, you can obtain assistance from the new-website wizard, see “Creating a Website with the Option User-defined” on page 218.

Distributed System with Two Websites

Several websites can be managed in a WCM system. The installed deployment systems on the servers are not limited to a single website. Since you can install multiple deployment systems – depending on the available data storage view – it is also possible to provide different views of various websites on a given server.

The following example shows a WCM system with a master Content server and two proxy Content servers. The two websites “CompanyIntranet” and “InternetSite” are managed in the WCM system.

Both the master Content server and proxy Content server 1 run in the context of a JSP engine or as a web application in an application server and can be used for editing and quality assurance of WCM objects by means of the Content client. The second proxy Content server is used for publishing the Production view of the website “InternetSite”.

The different data storage views (generated by the corresponding deployments systems) of the website “CompanyIntranet” are available on the following servers:

- master Content server: Edit view
- proxy Content server 1: QA and Production view

The data storage views of the website “InternetSite” are available on the following servers:

- master Content server: Edit view
- proxy Content server 1: QA view
- proxy Content server 2: Production view

Proxy Content server 2 is informed by proxy Content server 1 about changes to WCM objects in the website “InternetSite”. For this purpose, the Production view of the data is transmitted.

For the sake of simplicity, it is assumed that all the servers access the same data storage. The connections from the master Admin server to the other servers are not shown in the figure.

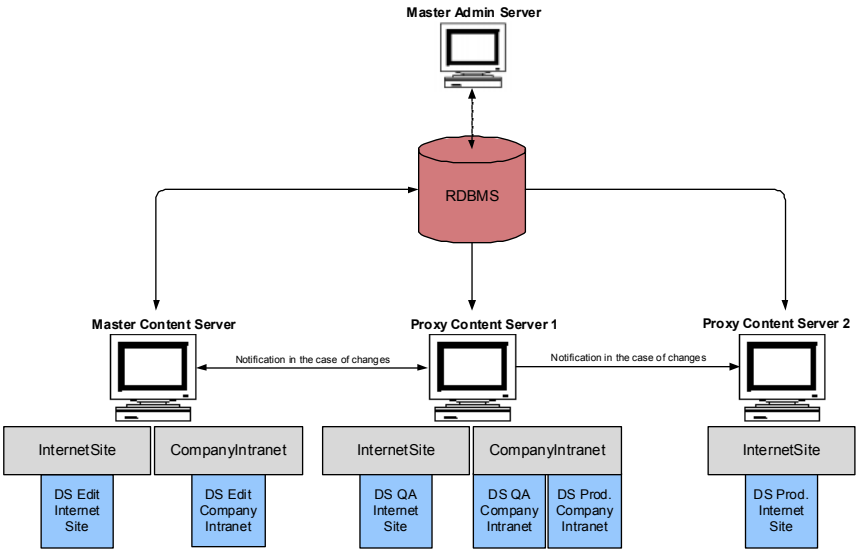


Fig. 10 – WCM system with two websites

A distributed system of this kind is created using of the option *User-defined installation* in the WCM installation program (see Livelink WCM Server Installation Manual). The new-websites wizard will support you when creating the websites, see “Creating a Website with the Option User-defined” on page 218.

Access Control

The access control functions in Livelink WCM Server make it possible to determine precisely who has access to which objects in a website. For each object of a website, you can determine which users may access the object and which rights these users have. For example, a user can read and change an object of the website, while having only read access to another object.

The access control facilities are not only extensive, but variable in use. They make it possible to construct widely differing access control systems, from a simple group administration to complex systems for security-relevant zones. Thus access control can be tailored precisely to the organization of your company.

A clear access strategy allows you to regulate object access without great effort and to adapt it to the responsibilities and requirements of the various users. When developing an access strategy for the WCM system, the following steps are important:

1. Adding users and organizing these users in groups and roles in the Admin client

   The organization of the users in groups and roles is a precondition for an access strategy. Roles are defined in terms of tasks, whereas groups are generally tied to organizational structures, such as departments or projects. Assigning rights to individual users should be the exception.

2. Defining and assigning functional areas in the Admin client

   Functional areas may be assigned to groups and roles (or individual users). The functional areas are used to determine which objects the users may add, check in, and check out, as well as which views, dialog boxes, and functions are available to them in the Content client.

3. Specifying default object rights for principals in the Admin client

   You can preset the object rights for groups and roles (or individual users). The object rights are used to determine which actions (read, change metadata, release, etc.) a user can by default perform on a WCM object to which the user is assigned.

4. Defining the access rights for the objects of the WCM-managed websites via the Content client

   For the individual objects of the website, you can then define which groups and roles (or individual users) get access and which concrete object rights are valid for this access.

   If you want to assign a workflow to the WCM objects and thus extend the predefined staging, you determine in the workflow definition which principals have the right to perform the individual workflow steps.

5. Assigning administration rights for the WCM system (Admin client).

   Access to the administration and configuration of the WCM system should be reserved to selected users. You can grant administration rights to users, groups, and roles.

In the following sections, these aspects of access control are explained in detail.

In addition to these features, *Secure Access* offers you the possibility of transferring the access control mechanisms to the web server or the JSP engine. In this way, you can create protected areas in your website, which are only accessible for registered users, even via the Internet (see “Access Control via the Web Server or JSP Engine with Secure Access” on page 78).

Users, Groups, and Roles

Like a network operating system, Livelink WCM Server allows you to assign the users of the WCM system to groups and to control access by assigning rights to these groups. If necessary, specific access rights can be given to individual users – this should, however, be the exception.

A role – like a user group – is a collection of users. Roles, however, are defined in terms of tasks, whereas groups are generally tied to organizational structures, such as departments or projects. Depending on activities, the roles in an organization may be defined in different ways. Some typical user roles that may be involved in editing a website are editors, graphics specialists, website administrators, and QA staff.

Specific access rights for objects can be defined for a role – just as they can for a group. Since roles are usually defined on the basis of tasks, it may be easier to assign access rights to a role than to a group, since editors, for example, need specific access rights, such as “Create” and “Change object”.

Use the Admin client to add and manage users, groups, and roles (see chapter 4 “User Administration”). Alternately, you can use the administration program of the connected LDAP directory service or Livelink. In the Admin client, the principals are assigned to the existing websites. This gives them access to the WCM objects via the Content client.

> **Note:** By organizing the users in groups and roles and assigning principals to websites, you create the preconditions for defining the access rights for the objects of your website(s). The actual access settings are properties of the WCM objects and are specified via the Content client.

Functional Areas

Via the functional areas, you control which functions are available to the users in the Content client. The functional areas perform two important tasks:

- They determine which types of objects the users may add, check out, and check in. Some functional areas, such as “Basic”, are by default assigned to object types. Only users that have the corresponding functional area can add, check in, and check out objects of this object type.
- They determine which views and dialog boxes are available to the user in the Content client. This way, you can specify exactly which actions the user is allowed to perform. For example, the Access rights dialog box is only displayed if the user has the functional area “Access rights dialog”. If users are not assigned this functional area via their group or role membership (or a direct assignment), they cannot view and edit the access rights of the WCM objects via the Content client.

Functional areas may be assigned to groups, roles, or individual users. This is done in the *User administration* view of the Admin client. Here, you can also add functional areas. For further information, see section “Managing Functional Areas” starting on page 150.

The default functional areas are assigned to the default object types. In the *Configuration* view of the Admin client, you can change these assignments and make further assignments for custom functional areas and object types (see “Object Type Settings” on page 231).

The following table shows the default functional areas available after the installation of the WCM system and their assignment to object types, as well as functions and views in the Content client. In some messages of the WCM system, the internal names of the functional areas are used. For this reason, they are also listed in the table.

Table 2 – Functional areas and object types

Functional area (internal Name)	**Default assignment to object type**	**Allowed view or function in the Content client**
Basic (VIP)	Excel document, GIF image, HTML page, JPEG image, PDF document, PNG image, PowerPoint file, Other, Topic, Compound object, Word document, XML document	Add, check out, and check in objects based on these object types
Advanced (ADVANCED)	Frame, Frame topic, HTML template, XML template	
Dynamic (DYNAMIC)	Assembled object, ASP page, ASP template, ASP topic, CGI script, Form template, JavaScript, JSP page, JSP template, JSP topic, PHP page, PHP template, PHP topic, XSLT document, XSLT template	
Form (FORM)	Form instance	
Workflow (WORKFLOW)	Workflow	Assign workflows to objects, remove workflow assignments

Functional area (internal Name)	Default assignment to object type	Allowed view or function in the Content client
Livelink (LIVELINK)	none	View the Livelink metadata dialog box
Intelligent templates (ITF)		Not used by default, required for compatibility with VIP 5e
Direct release (DIRECT_RELEASE)		Edit the option *Direct release* in the metadata
References dialog (REFERENCES)		View the References dialog box
Access rights dialog (ACCESS_RIGHTS)		View the Access rights dialog box
Log dialog (LOG)		View the Log dialog box
Filter standard (FILTER_STANDARD)		Use the standard filters
Filter edit (FILTER_EDIT)		Create and edit filters in the filter editor
View Subordinate objects (OBJECTLIST)		“Subordinate objects” view
View Object list (LISTVIEW)		“Object list” view
View My objects (FILTER_TODO)		“My objects” and “My work list” views

Functional area (internal Name)	Default assignment to object type	Allowed view or function in the Content client
View Template structure (TEMPLATE_STRUCTURE)	none	“Template structure” view
Import (IMPORT)		Use import functions
Search (COMI_SEARCH)		Use search functions

Since functional areas can be assigned to groups, roles, and individual users, overlaps between these assignments are possible as in the case of access rights. If a user has a specific functional area as a result of his/her group membership and a second functional area as a result of an individual assignment, then both functional areas are valid for that user. That means that the rights are “added up”.

Default Settings for Object Rights

In the Admin client, you can define preset access rights for WCM objects for each user, group, and role. These settings are called default object rights. If one of these principals is added to the list of those authorized to access an object in the Content client, these default settings are used as the initial settings for the access rights.

Default object rights are assigned via the user administration of the Admin client, see “Modifying User Assignments” on page 140 and “Modifying the Assignments of a Group or Role” on page 146.

The access rights are part of the metadata of the WCM objects and can be set individually for each object. The default object rights are only preset and can be edited at any time by users with the right “Change rights”.

Thus, changes to the default object rights of a principal in the Admin client do not result in changes to WCM objects. The changed default object rights will be displayed as presettings the next time a principal is assigned.

Access Rights for the WCM Objects

The access rights of an object are properties of the WCM objects and are part of the metadata. Via the Content client, you can allow access to a WCM object for groups, roles, and users, and define the detailed access rights. The default object rights of the principals defined in the Admin client are used as presettings.

> **Note:** Adding individual users to the access control list of an object should be the exception. Use the group and role organization as basis for your access control instead. Assigning individual users and making frequent changes to the access rights may result in confusing settings and unintentional overlaps in access control.

For detailed information on editing and analyzing access rights in the case of conflicting rights of users, groups, and roles, refer to the Content Client User Manual. Here, only the general procedure of developing an access strategy is described.

Rights for roles according to tasks

Different access rights are required for the different levels of staging (Edit, QA, and Production). An editor requires the right to change objects and metadata. Working in quality assurance requires above all the right to release. For reading objects in the Production view, only the right “Read (Production)” is necessary. Depending on the rights of the logged-in user, the Content client only offers selected functions.

The tasks users in the staging process are usually reflected in their assignment to a certain role. Users that are supposed to add objects to the website and edit them might belong to the role “Editor”. This role gets

the rights that are required for working as an editor: Create object, Change object, etc. Other users who work in quality assurance can be assigned to the role “QA”, which has the right to release objects.

The following figure illustrates the typical rights for the staging steps.

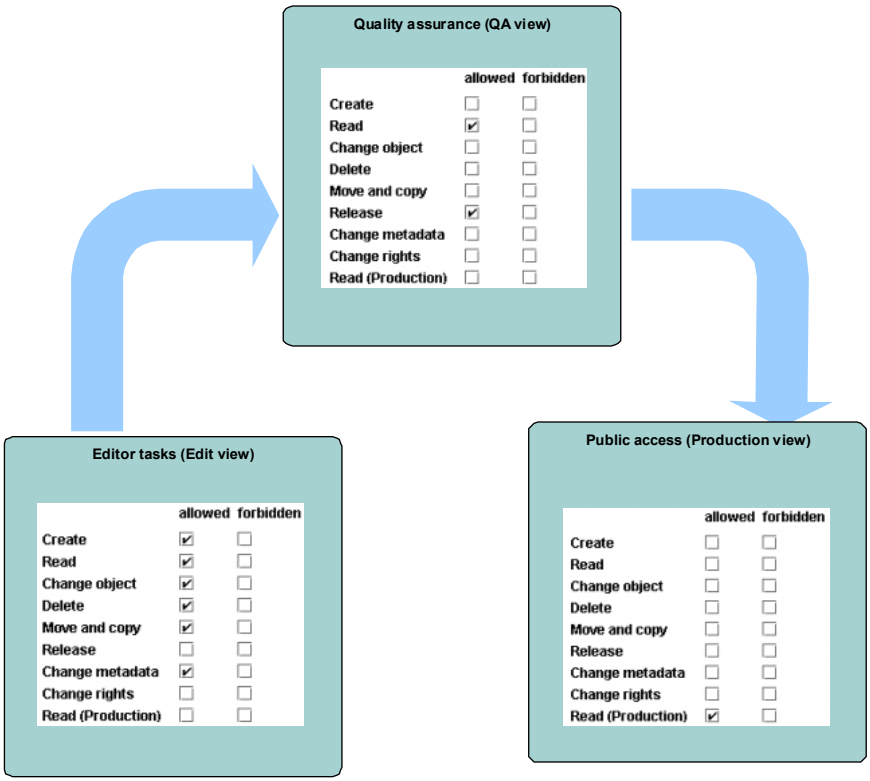


Fig. 11 – Access rights for Edit, QA, and Production

In addition to the tasks performed in the context of the staging, there are tasks that are usually performed by website administrators. These include, among other things, monitoring the rights structure of the website or managing the object structure, e.g. the object types and categories used. The object right “Change rights” should only be assigned to this role.

Rights for groups according to organizational structure

The Internet and intranet solutions of companies usually cover various areas that are maintained by different departments. By organizing the users in groups, you can control the exact rights of the different groups for the individual topics of the website. The group “Marketing”, for example, gets all access rights for the topic “Products”, whereas the group “Training” merely has read-only access here.

Note: The access rights structure for the objects of a website should be taken into consideration during the planning phase of website development to ensure that access rights and topic structure are well coordinated.

Access rights according to workflow

In addition to the staging, a workflow can be assigned to a WCM object. The individual steps of the workflow are assigned to certain users, groups, and roles. Only these principals are allowed to perform the respective workflow steps. Other principals that have sufficient object rights, but are not assigned to the respective workflow step, are denied access to the object.

When defining workflows for editing and quality assurance of your WCM objects, you must consider the combination of object and workflow rights.

Access Rights for the Admin Client

In the Admin client, you can assign administration rights to users, groups, and roles. Users with administration rights have access to the Admin client and can edit the components of the WCM system, such as servers, websites, deployment systems, and user information. It is possible to assign graded access rights. Thus, a user may only be allowed to view and edit parts of the administration. In this way, you can precisely delimit the areas of responsibility of the individual administrators.

Certain rights can only be assigned in combination with other rights, i.e. they include other rights. Example: if you assign a principal the right “Create, modify, delete configuration entry”, this principal will automatically be given the rights “Access to configuration” and “Change configuration entry”.

The following table provides an overview of the individual rights and their dependencies.

Table 3 – The individual administration rights

Right	Possible actions
Read access to user administration (API)	If a server agent is to read the user information, the user used for logging in the agent must have this right.
Access to user administration	Read access to the user information The tree items *Users*, *Groups*, and *Roles* in the *User administration* view are only displayed if the user has this right.

Right	Possible actions
Change principal	Change the settings of users, groups, and roles, as well as the assignments between these elements, e.g. assignment of a user to a group. To be able to change the assignment of principals to functional areas and websites, the right “Change assignment to website/functional area” is also required. Includes the right “Access to user administration”
Change assignment to website/functional area	Change the assignments of users, groups, and roles to websites and functional areas Includes the right “Access to user administration”
Create, modify, delete principal	Add, edit, and delete users, groups, and roles, as well as configure existing principals from an LDAP directory service as WCM principals Includes the rights “Change principal”, “Access to user administration”, “Change assignment to website/functional area”
Change administration rights	Edit the administration rights of principals Includes the right “Access to user administration”
Access to configuration	Read access to the configuration of the WCM system The *Configuration* view is only displayed if the user has this right.
Change configuration entry	Edit items in the *Configuration* view, including assignments between the elements, e.g. assignment of pools to servers Includes the right “Access to configuration” **Note:** Users who are not granted this right can nevertheless change the elements *Object types*, *Attribute sets*, *Object categories*, and *Converters* under *Websites* if they have the rights “Website administration” and “Access to configuration”.

Right	Possible actions
Create, modify, delete configuration entry	Add, edit, and delete items in the *Configuration* view, e.g. websites or deployment systems Includes the rights “Change configuration entry” and “Access to configuration”
Access to system administration	Read access to system administration and system overview The *System administration* and *System overview* views are only displayed if the user has this right.
Change system status	Log out users, change run levels of servers and websites, abort actions in progress on a server, and use commands in the *Tools* menu Includes the right “Access to system administration”
Website administration	Admin client: manage object types, attribute sets, and object categories; configure converters; change website run levels Content client: manage object types, attribute sets, and object categories For working in the views *Configuration* and *System administration* of the Admin client, the user additionally requires the rights “Access to configuration” and “Access to system administration”.

For information on assigning administration rights, refer to chapter 4 “User Administration”.

Access Control via the Web Server or JSP Engine with Secure Access

The component Secure Access of Livelink WCM Server enables the transfer of the access control used for editing a WCM object in the Content client to the web server or JSP engine. As a result, object-specific access control is possible for all objects in a website during productive operation (i.e. on the Internet as well).

Secure Access is implemented as servlet or filter. It runs in the JSP engine and ensures that all requests to the web server or JSP engine are checked to see whether an access right is necessary for the requested page. If so, the user must provide authentication for access to the page by logging in.

Preconditions for Using Secure Access

The following is required for using Secure Access:

- configuring the HTTP server and the JSP engine for Secure Access. For more information, refer to the Livelink WCM Server Installation Manual.
- activating Secure Access for the Content servers whose deployment systems are used to publish the data to be protected. This is done via the Admin client in the settings of the respective server (see section “General Server Settings” on page 176).
- configuring the directories that are to be monitored by Secure Access (the so-called Secure Access assigned paths). This is done in the assignments of the desired Content server (see section “Managing Paths for Secure Access” on page 186).

  This is also where you make further settings for Secure Access. For detailed information on the individual settings, refer to the Admin client's online help.

How Secure Access Works

Secure Access is implemented as servlet or filter and runs in a JSP engine. If Secure Access is active, the following actions are performed:

1. When a page is requested from the web server or JSP engine via a browser, Secure Access intercepts this request and checks whether it is addressed to one of the configured protected directories.
2. If this is the case, the URL of the respective object is sent to the Content server for which the respective path was configured. This must be the server on which the associated deployment system is installed.
3. The server checks the access rights of the associated WCM object and informs Secure Access whether the object can be read by all users (access settings “Read” or “Read (Production)” for “World”) or only by certain WCM users.
4. If unlimited access to the object is not allowed, the user must enter a user ID and password for access to the WCM system in a Login dialog box in the browser.

   As an alternative to logging in via the browser, the login information of the Windows operating system may also be used for authenticating the user. This is possible if you operate the WCM system in a Windows domain and use MS Internet Information Server as the web server and MS Internet Explorer as browser. To enable this login procedure, you must select the login method *ntlm* in the settings of the Secure Access paths.
5. After the login in the browser, the Content server sends the user information to the Admin server of the WCM system. This server checks the information and returns a login confirmation or rejection to the Content server.

6. If the login of the user has been successful, the pages can be displayed via the HTTP server and the user can view the object in the browser.

The following figure illustrates the procedure of checking accesses with Secure Access.

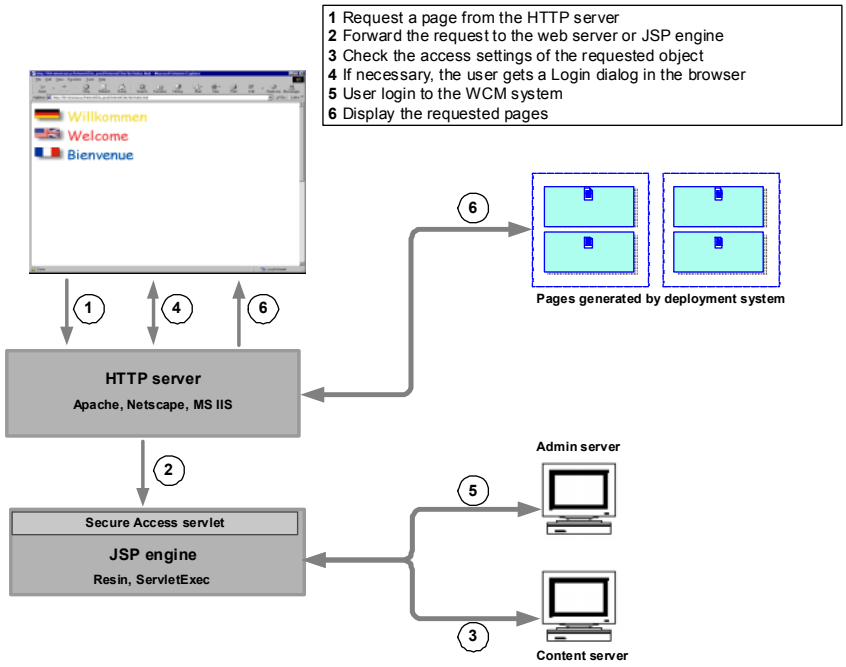

1 Request a page from the HTTP server
2 Forward the request to the web server or JSP engine
3 Check the access settings of the requested object
4 If necessary, the user gets a Login dialog in the browser
5 User login to the WCM system
6 Display the requested pages
Willkommen
Welcome
Bienvenue
Pages generated by deployment system
HTTP server
Apache, Netscape, MS IIS
Secure Access servlet
JSP engine
Resin, ServletExec
Admin server
Content server

Fig. 12 – Overview of Secure Access

Notes

- Secure Access only protects the files generated by the deployment systems. This protection can be used for the Production view as well as for the Edit and QA views.

It is not necessary to protect dynamic deployment systems with Secure Access. The servlets used for the dynamic deployment are responsible for access control.

- In the settings of the paths for Secure Access, you can specify that the login data of the user is saved in a cookie. This cookie ensures that the user does not have to log in again when, for example, starting the Content client via the browser to edit objects after viewing protected pages. This cookie is also used by other components of the Livelink WCM Server, e.g. the Portal Manager API. This guarantees a single sign-on.

  When adding paths for Secure Access, you can configure how long the cookie is to remain valid (parameter *Cookie timeout*). If this parameter is not set, the cookie is by default deleted when the browser is closed.

- If the user enters a wrong password during login, the login dialog box opens again at least twice. Thus, it is possible to enter the password again.

  If the user enters a wrong user ID (name), the browser must be closed and restarted before the user can log in again.

- When many users simultaneously access the pages of a protected directory, this results in a high number of logins to the WCM system. To process these logins, many connections between the Content servers and the Admin server are required. To avoid communication bottlenecks, increase the maximum number of connections in the Admin server's pool. To do so, select *Configuration* → *Pools* → *WCM* → *{Admin server name}* → *Connections* tab. By configuring a cookie timeout (see above), you can reduce the number of logins.

- Secure Access also sets up connections to the following servers without using the pool mechanism:
  - to the Content server running with Secure Access in the context of a JSP engine or as a web application in an application server. Secure Access reads its configuration from this server.
  - to all Content servers for which Secure Access is active and which use the same profile (parameter *Web server* in the Secure Access configuration).

Unicode with Livelink WCM Server

Due to the growing internationalization of companies, it has become necessary to publish websites not only in Western European languages, but also in Eastern European and Asian languages. This can be realized with the Unicode standard for displaying characters. The following sections offer a general introduction to Unicode and a description of the basic procedure when configuring Livelink WCM Server for Unicode.

What is Unicode

Computers process letters and other characters by assigning a number (code) to them. The development of information technology has been dominated by the English language. For this reason, the most common encoding systems, like ASCII or its extension Latin-1 (ISO-8859-1), only contain character codes for the letters and special characters of Western European languages. These character codes cannot be extended. The *Unicode* standard was developed to also display Eastern European and Asian languages. Theoretically, it can be expanded indefinitely and at present comprises several thousand characters. The characters 0–255 include the ASCII and Latin-1 codes.

Note: For detailed information on Unicode, refer to http://www.unicode.org.

To be processed, the characters codes are converted into byte sequences. This is called *encoding*. In the case of ASCII and Latin-1 encoding, the character code is mapped 1:1 to the byte sequence. Each character code is represented by 1 byte (8 bits).

For the encoding of Unicode characters, however, more than 8 bits are required. For this reason, 16-bit character representations are used for Unicode characters. For displaying characters that could be represented by 8 bits according to Latin-1, a 16-bit representation would be unnecessary, as saving texts encoded this way would require too much storage space. Thus, the encoding *UTF-8* only uses more than 8 bits for a character if necessary. The UTF-8 standard can thus be used universally for all characters, but only needs little more transmission capacity if the text mainly consists of ASCII characters.

For displaying UTF-8-encoded pages on the Internet, the encoding of the pages must be specified in the source text of the document. For HTML pages, this is done by means of the tag `<meta http-equiv="content-type" content="text/html;charset=UTF-8">`, for JSP pages, the page directive `<%@page contentType="text/html;charset=UTF-8" %>` must be added.

Configuring Livelink WCM Server for UTF-8

When planning your WCM system, you should decide whether to always use the Latin-1 character set (ISO-8859-1) or the Unicode character set (UTF-8 encoding). If you only use Western European languages on your website(s), you do not have to use Unicode. Latin-1 is completely supported by all common web applications. However, if you require additional language support, you should opt for UTF-8 right from the beginning, even if you do not need it until later.

The different components of the WCM system must be configured to use UTF-8. It is important that all components use the same encoding. Otherwise, errors might occur when displaying HTML pages, generating pages, etc.

- **RDBMS:** When configuring the RDBMS, you can determine that UTF-8 encoding is to be used for data of type “String”.

  You should configure the database for UTF-8, even if Latin-1 encoding is used in your website. The additional memory space required for UTF-8 encoding is relatively small. This way, you do not have to migrate the database later.

  For information on the configuration of the RDBMS, refer to the Livelink WCM Server Installation Manual and to the documentation of the manufacturer.

- **Website:** When creating a website, you can determine whether the content is to be UTF-8-encoded (see “Step 1 – Specify Website Name and JDBC Pool” on page 207). If you do not activate this option, Latin-1 encoding is used by default.

If you select UTF-8, the following tag is automatically inserted in the head element of the HTML page when the page is generated: `<meta http-equiv="content-type" content="text/html; charset=UTF-8">`. When the WCM tags in the page content are replaced, the characters will be UTF-8-encoded.

> **Note:** To also activate UTF-8 for JSP pages, you must add the page directive `<%@page contentType="text/html;charset=UTF-8" %>` to the respective pages and templates. This is not done automatically during page generation.

- **Attributes and properties:** For the names of attributes from attribute sets and properties from object categories, only ASCII characters may be used.
- **Editors for website content:** If UTF-8 encoding was activated for the website, only editor programs supporting UTF-8 may be used.
- **Content client:** When installing a Content server that runs in the context of a JSP engine or as a web application in an application server, or when generating a web application for such a Content server, you can specify which encoding is to be used for the Content client.

  > **Note:** The Content client (Classic) always uses UTF-8 encoding.

  - Setting the Content client to Latin-1: The Content client can only display and manage Latin-1 characters. Use this setting if the RDBMS and the website are also set to Latin-1.

- Setting the Content client to UTF-8: With this option, you can use the Content client for editing websites with content and metadata encoded in UTF-8.

  Notes:

  The encoding for client and website must be the same. Otherwise, special characters will not be displayed correctly when WCM tags are replaced.

  If you use an application server supporting the servlet API 2.2 only, Unicode characters cannot be used in the metadata of the WCM objects. Thus, in this case, you must set the Content client and the website to Latin-1 encoding.

- **URLs and web server:** The URLs generated by Livelink WCM Server (to be more precise: the path part of the URL) are always Latin-1-encoded, as this is expected by the majority of web servers. If the web server is set to UTF-8, only ASCII characters (i.e. no special characters) may be used in the file names of the generated pages. The file names are specified by means of the metadata item “Suggested file name” in the Content client.

  Depending on the product used, it might be necessary to specify the encoding set for the Content client in the configuration of the web server. For information on configuring web servers, refer to the Livelink WCM Server Installation Manual and to the documentation of the manufacturer.

- **Secure Access:** In the configuration of the Secure Access servlet or filter, you specify which encoding is to be used for reading the request parameters. This must correspond to the encoding of the protected pages. If you have created the website with UTF-8 encoding, you must also set UTF-8 for Secure Access.

  For information on the configuration of Secure Access, refer to the Livelink WCM Server Installation Manual.

WebDAV with Livelink WCM Server

WebDAV stands for *Web-based Distributed Authoring and Versioning*. It is a set of extensions to the HTTP protocol which allows users to collaboratively edit and manage files on remote web servers. Livelink WCM Server enables you to use WebDAV clients for editing WCM objects.

> **Note:** For information on supported clients and web servers for WebDAV, refer to the Release Notes for Livelink WCM Server.

For using WebDAV, the following requirements must be met:

- The WebDAV support of Livelink WCM Server is based on a servlet. For this reason, the Content server used for accessing the WCM objects must run in the context of a JSP engine or as a web application in an application server.
- An HTTP server must be installed on the computer hosting the Content server. For information on configuring the HTTP server for WebDAV, refer to the manufacturer's documentation.
- The WCM system must be configured for WebDAV. The required steps are described below.

Configuring the WCM System for WebDAV

The following configuration steps are required to configure the WCM system for WebDAV:

1. Assign the JDBC pool used to the `VipDAVLockRepository`.
2. Configure the servlet mapping in the JSP engine used.
3. Set up a WebDAV deployment system.
4. Assign the `VipDAVApplication` to the Content server and configure the application.

Step 1 – Assign the JDBC Pool to the VipDAVLockRepository

The VipDAVLockRepository locks objects for editing and saves the changes made to the objects. For this purpose, you must assign the JDBC pool used to access the database in which the WCM objects are stored to the repository.

To assign a JDBC pool to the VIPDAVLockRepository:

1. Launch the Admin client.
2. Select *Configuration* → *Repositories* → *VipDAVLockRepository*.
3. Choose *Parameters* → *store* → *VIPDAV_LOCKSTORE*→ *poolname* → *default*.
4. In the right window pane, enter the name of the JDBC pool as the value of the default parameter.

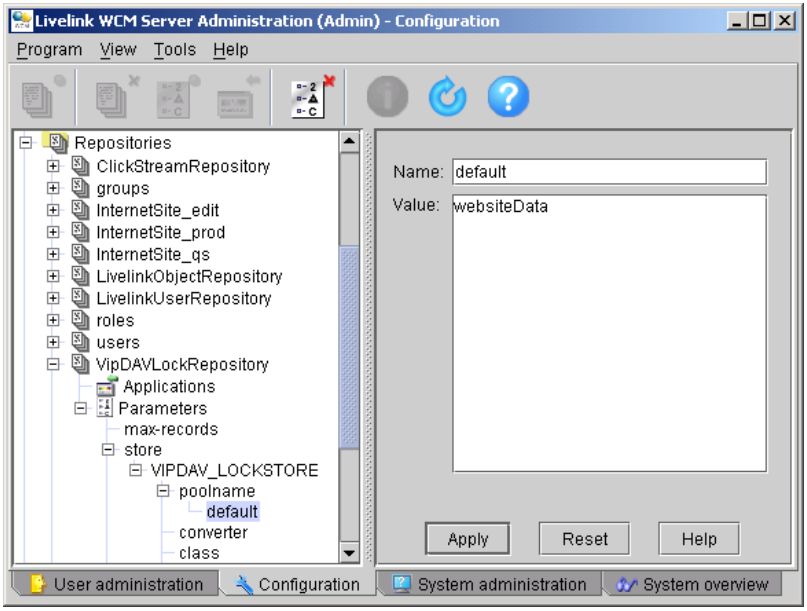


Fig. 13 – Configuring the JDBC pool for WebDAV

The JDBC pool you enter in the `default` parameter is used by all according Content servers for accessing the database.

If the Content servers access separate databases, you must configure the respective JDBC pools. To do so, add a node named *server* below *store* → *VIPDAV_LOCKSTORE*→ *poolname*. Below this node, add parameters for the individual servers. The parameter name corresponds to the server name, the parameter value is the name of the respective pool.

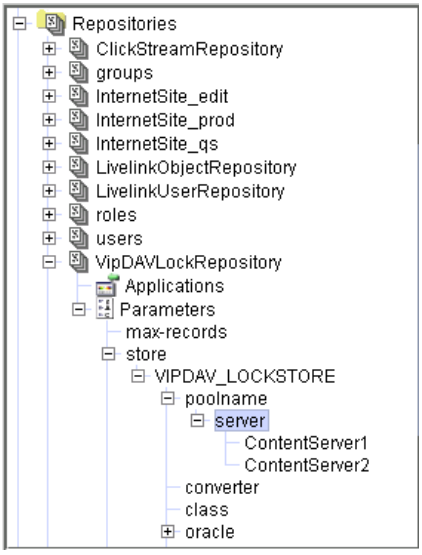


Fig. 14 – Configuring multiple JDBC pools for WebDAV

5. Click the *Apply* button.

Step 2 – Configure the Servlet Mapping

> **Note:** This configuration step is not required if the Content server used runs as a web application in an application server.

Enter a servlet mapping for the WebDAV servlet of Livelink WCM Server in the configuration of the JSP engine you use. If you work with Resin, for example, the mapping looks as follows:

```
<servlet-mapping url-pattern='/vipdav/*'
      servlet-name='de.gauss.vip.webdav.VipDAV'/>
```

Step 3 – Set up a WebDAV Deployment System

To add a WebDAV deployment system:

1. Launch the Admin client.
2. Select *Configuration* → *Deployment systems*.
3. Choose *New deployment system* on the context menu or click the corresponding icon.

   Icon for adding a deployment system

   The wizard for new deployment systems starts.
4. Follow the instructions of the wizards. Please note the following:
   - In the first window of the wizard, select the category *WebDAV deployment system*.
   - In the second window of the wizard, select the Content server as server which is used to access the objects. This Content server must run in the context of a JSP engine or as a web application in an application server.

WebDAV URL

The URL of the deployment system “InternetSite_edit” may look as follows:

http://wcmserver.company.example/vipdav/InternetSite_edit

This results in the following WebDAV URL for accessing the objects of the website “InternetSite”:

http://wcmserver.company.example/vipdav/InternetSite_edit/InternetSite

Step 4 – Assign and Configure the `VipDAVApplication`

Assign the `VipDAVApplication` to the Content server used for accessing the WCM objects.

1. Launch the Admin client.
2. Select *Configuration* → *Servers* → *{name of the Content server}* → *Applications*.
3. Choose *Assign application* on the context menu or click the corresponding icon.

   Icon for assigning an application

4. Select the `VipDAVApplication` from the list.
5. Click the *OK* button.

Using the parameters of the `VipDAVApplication`, you can specify WebDAV settings. For detailed information on the individual parameters, refer to the Portal Manager API Programmer's manual and the Admin client's online help.

CHAPTER 3

Working in the Admin Client

The Admin client is the central point of configuring and administering the WCM system and managing the WCM user information.

The Admin client is available on all hosts on which a WCM system is installed. It can also be installed separately on computers where there are no other components of Livelink WCM Server. For more information, refer to the Livelink WCM Server Installation Manual. Alternately, you can start the Admin client can as a web application – without installing it locally (see section “Using the Admin Client as a Web Application” on page 117).

Logging In and Out

The Administration server must be running before you start up the Admin client. For certain configuration operations, such as creating websites, the other servers must also be running.

An installed Admin client is called by the file **adminClient.bat** (Windows) or **adminClient.sh** (Unix). These files are located in the subdirectory **\admin** of the WCM installation directory. To start an Admin client's web application, open a browser and go to the URL of the web application's start page (e.g. **http://wcmserver.company.example/wcmadminclient/index.html**).

Immediately after installation, the only user with administration rights is the one you entered during installation.

Note: If you are working with an LDAP system, the WCM administrator must already be equipped with the mandatory attributes of the WCM object classes. Only in that case, the administrator is able to access the Admin client. For notes on integrating an LDAP directory service, refer to the Livelink WCM Server Installation Manual.

To log in to the Admin client:

1. Launch the Admin client.

   The Login dialog box opens.

Fig. 15 – Logging in to the Admin client

2. Enter your user ID and the corresponding password.
3. Click the *Login* button.

   When you first log in to the WCM system, you are asked to change your password.

> **Note:** User ID and password are case sensitive. For Livelink WCM Server, “administrator” and “Administrator” are two different users.

Expiration interval

If you do not work in the Admin client for a longer period of time, the connection to the Admin server is interrupted. If you want to resume your work, you will have to log in again. The interval after which the connection to the Admin server is interrupted can be specified in the Admin server settings (*Administration* tab, *Expiration interval* parameter).

Logging in with a different user ID

While working in the Admin client, you can log in with a different user ID. Choose *Re-login* on the *Program* menu. The main window of the Admin client builds up again in the language of the corresponding user.

Current login information

To view information on the user currently logged in to the Admin client and on the selected Admin server, choose *About* on the *Help* menu.

Quitting the program

To exit the Admin client, choose *Quit* on the *Program* menu. The connection to the Admin server will be terminated. This may take some time.

The User Interface of the Admin Client

Once you have successfully logged in, the Admin client user interface appears. The window is divided into different areas.

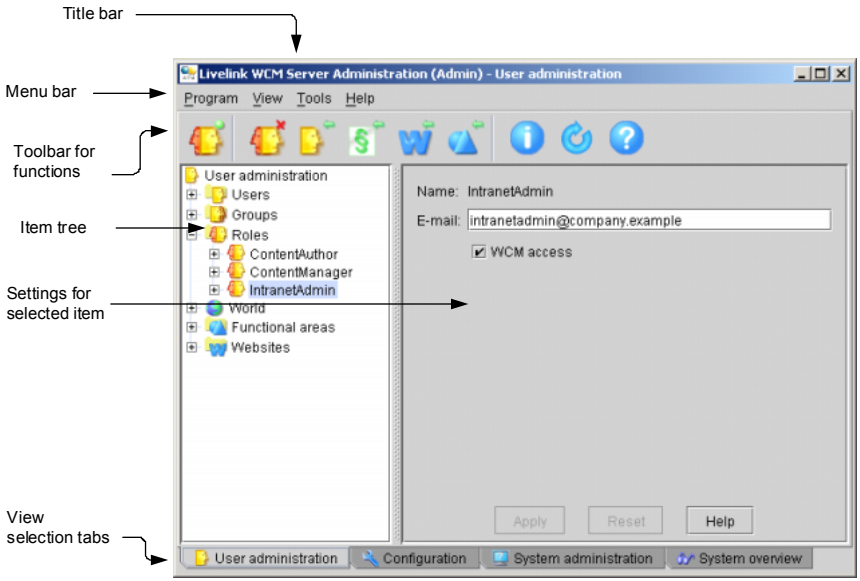


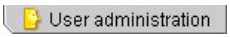
Fig. 16 – The user interface of the Admin client

Note: The configuration of a distributed WCM system can be edited via different Admin clients. Subsequently installing or deinstalling components or importing websites also changes the configuration. After each configuration change, refresh the view in the Admin client by clicking the appropriate icon, or restart the client. This loads the current configuration. Otherwise, you might make changes on the basis of an out-of-date configuration which causes error messages.

The Views

The Admin client has four tabs on which you can make various settings.

Table 4 – Functions in the four Admin client tabs

Tab	Function
	Manage users, groups, and roles (collectively known as *principals*); create assignments between the principals themselves and between principals and websites or functional areas See chapter 4 “User Administration”
	Configure pools, connection types, servers, websites, deployment systems, server agents, utilities, repositories, applications, and Search servers (if installed) See chapter 5 “Managing Pools and Connection Types” chapter 6 “Managing Servers” chapter 7 “Managing Websites” chapter 8 “Managing Deployment Systems” chapter 9 “Managing Agents and Utilities”
	Manage active servers and websites as well as active users, including report and trace functions, license management; manage Search servers (if installed) See chapter 10 “System Administration”
	Graphical overview of the components and connections of the WCM system See chapter 11 “System Overview”

Choose the respective command in the *View* menu or click one of the tabs to switch between the views. The active view is displayed in the title bar.

Important! The number of tabs and functions displayed depends on the administration rights you have. The administration rights are included in the assignment of users, groups, and roles. For an overview of the individual administration rights and the respective functions, refer to section “Access Rights for the Admin Client” on page 75.

Selecting Functions

There are different ways of selecting functions in the Admin client:

- from the toolbar
- from the context menu
- from the menu bar

The toolbar

Depending on the current view (e.g. *Configuration*) and item (e.g. *Websites* → *InternetSite*), the toolbar contains all the functions that are available for this main item. If you choose one of the subitems (e.g. *Configuration* → *Websites* → *InternetSite* → *Proxy Content servers*), the toolbar icons for the unavailable functions become dimmed and inactive.

Fig. 17 – Icons available for a selected website

Fig. 18 – Icons available for *InternetSite* → *Proxy Content servers*

The context menu

All functions that you can select from the toolbar are also available from the context menu. Simply mark the desired item, then right-click on it. Like the toolbar, the context menu offers only those commands which are available for the current item.

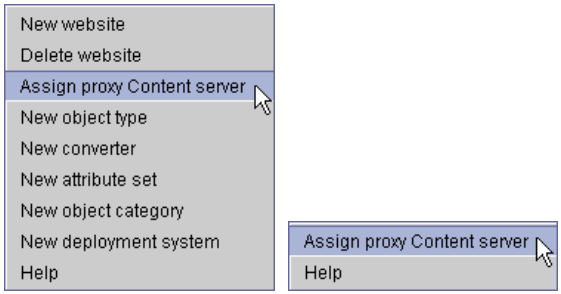


Fig. 19 – Context menus for a selected website and for *InternetSite* → *Proxy Content servers*

The menu bar

The menu bar contains the commands for exiting the program and calling the online help, as well as special commands that are not available from the toolbar or the context menu. These special commands include:

- Menu *Program* → *Re-login* (see section “Logging In and Out” on page 95)
- Menu *Program* → *Settings* (see section “General Settings of the Admin Client” on page 116)
- Menu *Tools* → *Create web application for Admin client* (see section “Creating a Web Application for the Admin Client” on page 119)
- Menu *Tools* → *Collect orphan objects* (see section “Reassigning Orphan Objects” on page 243)

- Menu *Tools* → *Deploy resources* (see section “Deploying Resources” on page 122)

All commands in the Admin client menus can also be selected by means of *keyboard shortcuts*. To update the entire view, for example, press F5.

The keyboard shortcuts are shown after the relevant commands in the menus.

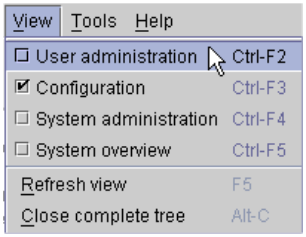


Fig. 20 – Menu commands and keyboard shortcuts

Editing Items in the Admin Client

The following section gives you a brief introduction to working with the Admin client. The following procedures will be explained:

- selecting items
- using filter functions for displaying items
- adding items
- deleting items
- editing the basic settings of items
- creating and removing assignments

Selecting Items

Depending on the selected view, the relevant items are displayed in the tree on the left, e.g. the *Configuration* view shows the pools, connection types, websites, etc.

To expand a main item, such as *Pools*, to show its subitems, click the plus sign ⊞ in front of the item. To collapse the list of subitems again, click ⊟.

> **Note:** To collapse the complete item tree, use the appropriate command in the *View* menu.

If you select a main item in the tree, a list of the relevant subitems is displayed in the right window pane, e.g. a list of the websites.

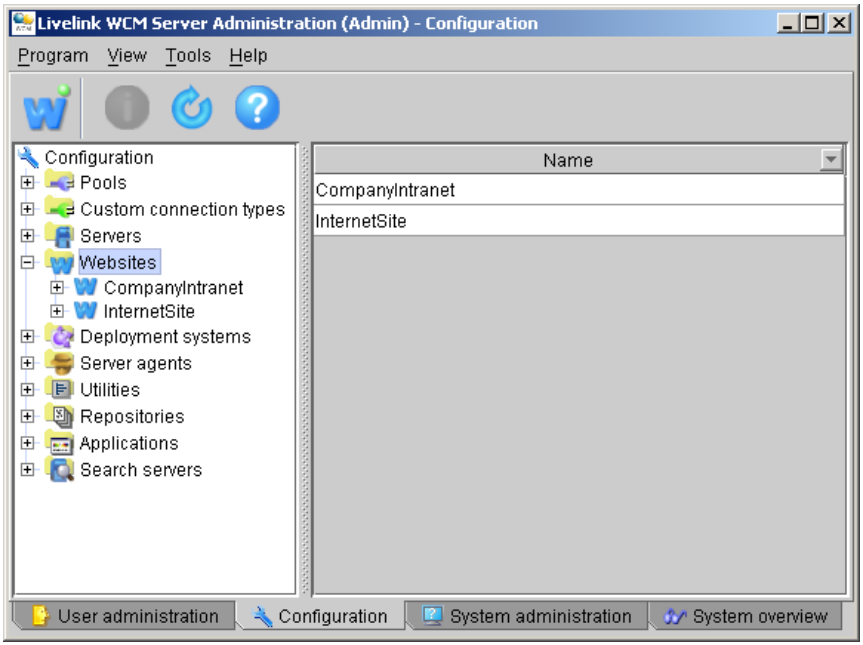


Fig. 21 – Website list

Tips:

Double-clicking one of the items in the list, e.g. the website “InternetSite”, takes you straight to the settings for that item.

By clicking on the header row of a column, you can sort the items in the list according to the criterion in this column. For example, clicking the *Name* column sorts the items in ascending alphabetical order. To reverse the sort order, click the header row again.

Using Filter Functions

The number of principals (users, groups, and roles) that are managed in a WCM system, an LDAP directory service, or in Livelink may be very large. Loading and displaying all principals may thus take a long time. For this reason, filters are provided in the user administration for all principals in order to restrict the number of items displayed. In the Admin client settings, you can also specify how many items are to be loaded for display, see section “General Settings of the Admin Client” on page 116.

The fields for the filter criteria are displayed in the right window pane when you click one of the items *Users*, *Groups*, or *Roles*.

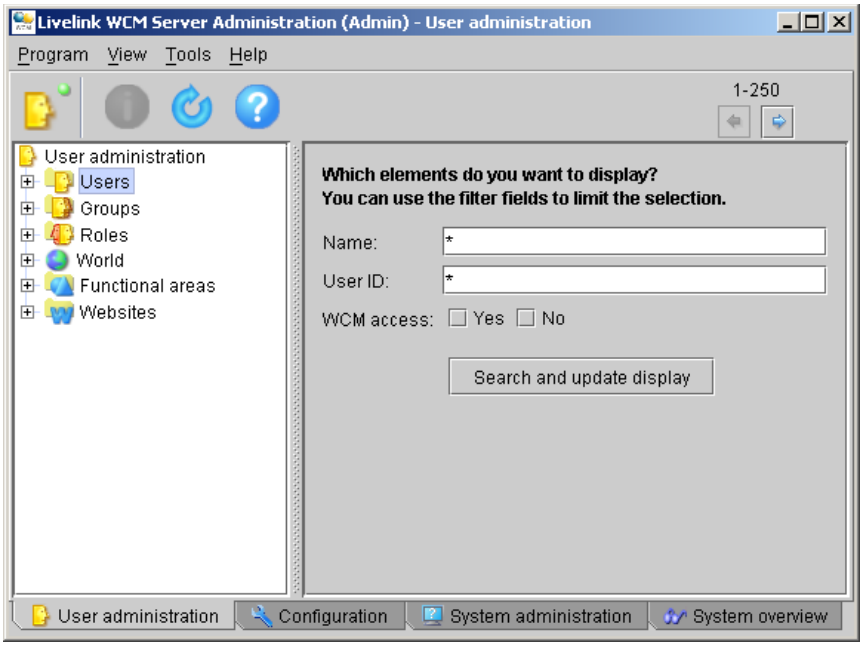


Fig. 22 – Filter criteria for displaying users

To select the items to be displayed:

1. Enter the criteria for the display filter. You can use the following search criteria:
   - name of the principal

     If the user information is stored in a Livelink system, you can only search for the last name of a user.
   - user ID
   - WCM access
   - LDAP position and LDAP search mode (recursive or not)

You can use the asterisk (*) character as a placeholder in searches. The asterisk replaces any number of characters before, after, or inside a search string.

2. Click the *Search and update display* button.

   The tree displayed on the left is updated according to the search results. For example, after a search for individual users, the *Users* item contains only the users found in the search.

3. To display all items again, delete the filter criteria. Again, click the *Search and update display* button.

Adding Items

To add an item, such as a deployment system:

1. Select the desired view, e.g. *Configuration*.
2. In the tree on the left, mark the node to which you want to add an item, e.g. *Deployment systems*.
3. Right-click the node, then choose the command for adding an item on the context menu, e.g. *New deployment system*.

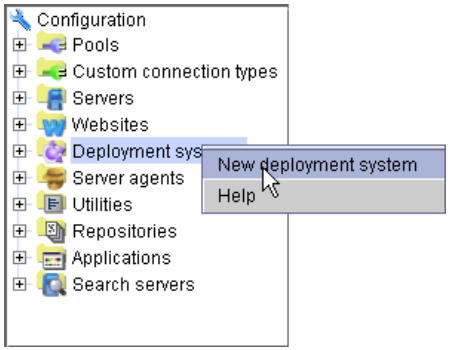


Fig. 23 – Adding an item via the context menu

Alternately, you can click the corresponding icon.

Icon for adding a deployment system

Deleting Items

To delete an item, such as a user:

1. Select the desired view, e.g. *User administration*.
2. Mark the item, e.g. an individual user, in the tree on the left.
3. Right-click the item, then choose the appropriate Delete command on the context menu, e.g. *Delete user*.

   Alternately, you can click the corresponding icon.

Icon for deleting a user

When you delete an item, it is automatically deleted from all relevant assignments. So in our example, the deleted user is no longer listed in the assignments of a group. This automatic update of assignments is performed throughout the entire Admin client.

Editing the Basic Settings of Items

Every item has a number of *basic settings*, e.g. the name of a principal or the basic URL of a website. If you have expanded the tree down to an individual item, such as a group, the basic settings for that item are shown in the right window pane. In the case of a group, this would include the e-mail address.

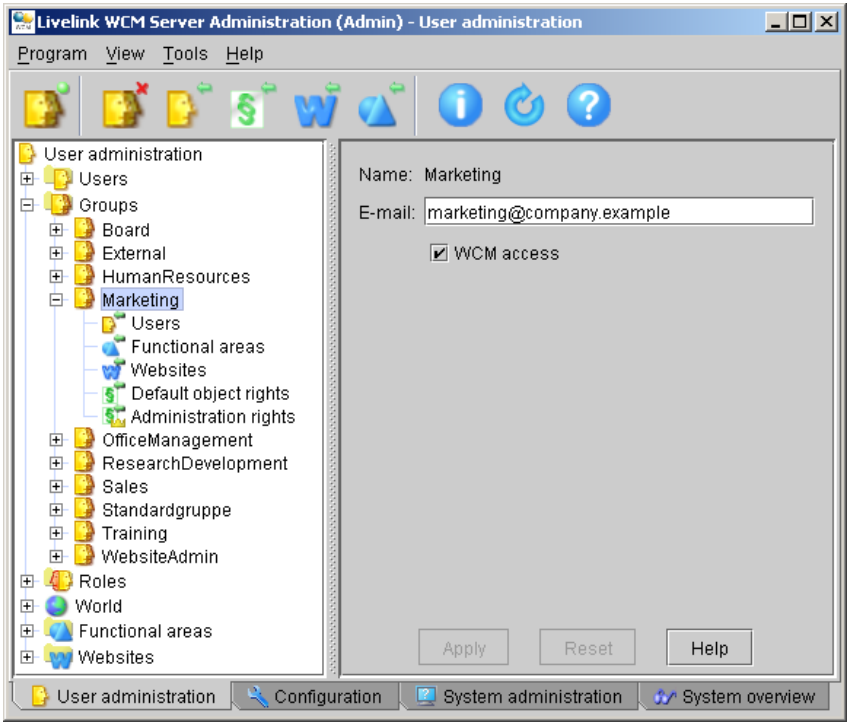


Fig. 24 – Basic settings of a group

To change an item's settings:

1. Make the desired changes in the right window pane.
2. Click the *Apply* button.

Editing Assignments of Items

Assignments represent relationships between items – for example, you can assign individual users to a group or create an assignment between a proxy Content server and a website.

All the assignments of an item are displayed when you open the item in the tree. In case of a group, these include the assigned users or websites.

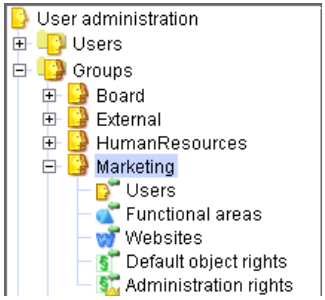


Fig. 25 – Assignments of a group

Creating Assignments

To create an assignment between two items:

1. Mark the desired item in the tree on the left, e.g. the group to which you want to assign a user.
2. Right-click the item, then choose the appropriate command on the context menu, e.g. *Assign users*.

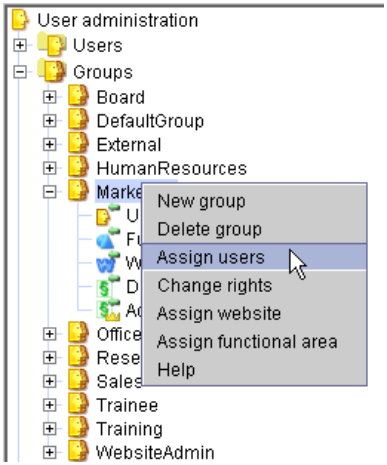


Fig. 26 – Assignment using the context menu

Alternately, you can click the corresponding icon.

Icon for assigning a user

3. In the selection dialog box, select the desired item for the assignment.

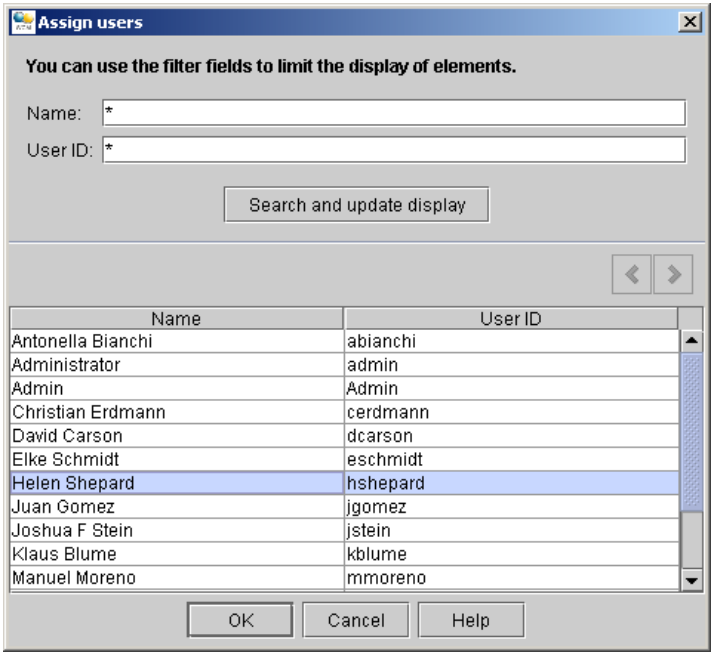


Fig. 27 – Assigning a user to a group

When assigning principals, you have the possibility of using the filter functions to restrict the number of principals displayed. By using the search fields, you can quickly find a specific principal (see “Using Filter Functions” on page 104).

Use the arrow icons to scroll through long lists. You can specify the number of items displayed in the configuration of the Admin client, see section “General Settings of the Admin Client” on page 116.

4. Click the *OK* button.

Removing Assignments

To remove the assignment between two items, e.g. between a group and a user:

1. Open the assignments for one of the two items, e.g. the group “Marketing”.
2. Mark the desired assignment in the tree on the left, in our example *Users*.

   The right window pane shows the users belonging to the group.
3. In the right window pane, right-click the desired user.
4. Choose the command for removing the assignment on the context menu, in this case *Remove user assignment*.

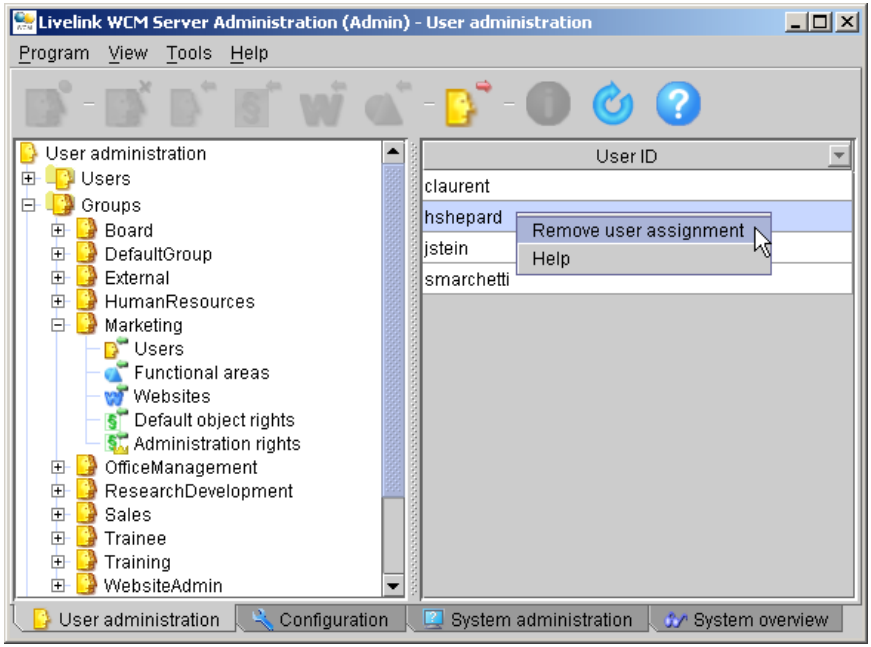


Fig. 28 – Removing assignments using the context menu

Alternately, you can click the corresponding icon. All icons for removing assignments have a red arrow.

Icon for removing a user's group assignment

Two Ways to Edit Assignments

An assignment creates a relationship between two items of a WCM system. The information about these assignments is available through both items of the assigned couple – allowing you, for example, to view and edit assignments between proxy Content servers and websites either via the website or via the relevant Content server.

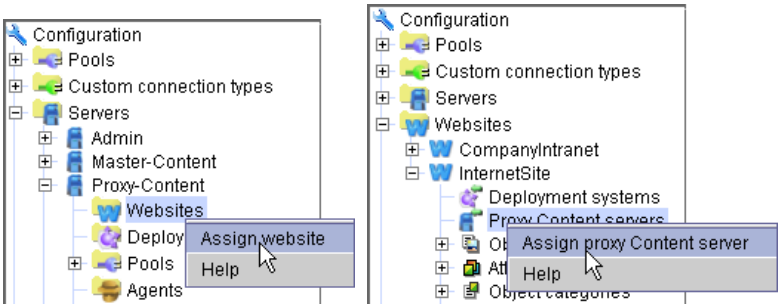


Fig. 29 – Two ways to assign a server to a website

When removing assignments, it is also possible to start from either item of the assigned couple.

This information redundancy applies to all assignments that you can create with the Admin client. In most cases, this documentation describes only one of the ways to create or remove assignments.

Overview of all Assignments for an Item

The Admin client offers you the facility of displaying all direct assignments of an item in an information window. Mark the desired item, e.g. an individual user or a website, then click the info icon in the toolbar. To close the information window, click the icon again.

Icon for opening or closing the information window with all the assignments for an item

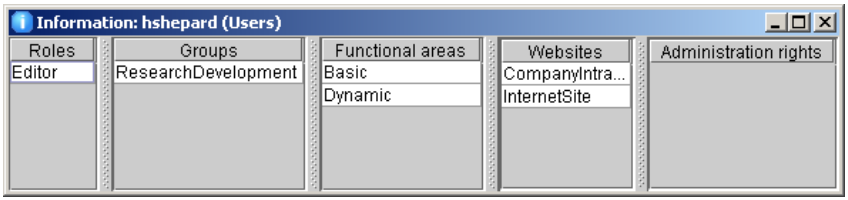


Fig. 30 – User assignments overview

The information window has a separate column for each type of assignment. You can double-click the entries in the columns. The view changes and the Admin client shows you the settings for the item that you double-clicked. For instance, if in the example above you double-click on the entry “Editor” in the “Roles” column, the role “Editor” is marked in the item tree. The information window now shows an overview of the assignments for the role “Editor”. This enables you to find out very quickly which other users are also assigned to this role.

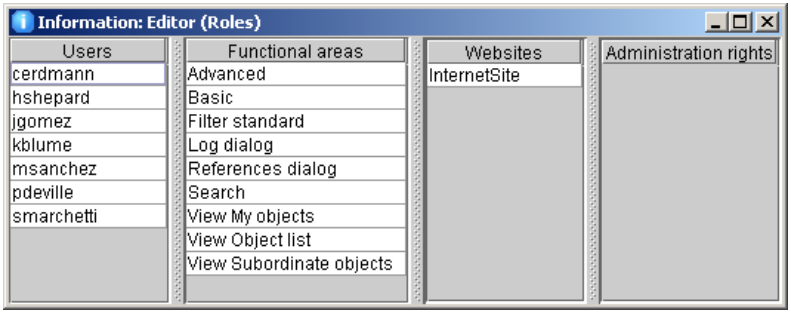


Fig. 31 – Assignments for a role

Double-clicking the user (“hshepard”) takes you back to the assignments for that user.

Managing Other Products of Livelink WCM Server

The Admin client is the central point of administration for all components of Livelink WCM Server which require appropriate licenses. Depending on the way the other products work, they are integrated at various levels in the Admin client.

- The runtime environment of the Portal Manager API is supplied with Livelink WCM Server, as the API is required for using the Content client. The Portal Manager API as development platform can be used to implement dynamic websites and enterprise portals.

  The Portal Manager API items *Applications* and *Repositories* are managed in the *Configuration* view of the Admin client. The configuration of this product is described in the relevant manual.

- Search servers (Content Miner, Lucene, and Livelink) offer intelligent search functions for websites. Configuration and administration of Search servers are handled via separate nodes in the *Configuration* and *System administration* views. These nodes are only visible if Search servers are installed. How to configure and manage these products is described in the relevant manuals.

General Settings of the Admin Client

In the Admin client's settings, you select an Admin server and configure the display of items.

To open the settings of the Admin client, choose *Settings* on the *Program* menu. The *Admin client settings* dialog box opens.

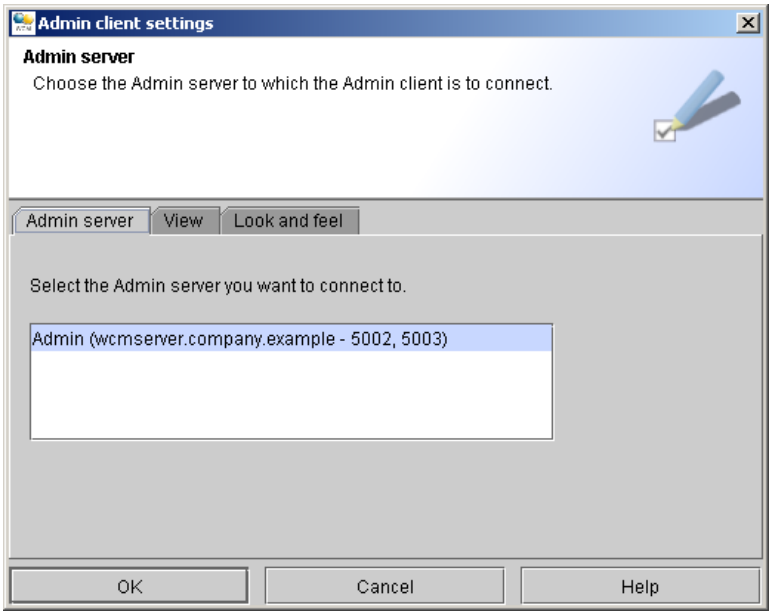


Fig. 32 – General settings of the Admin client

You can make the following settings:

- *Admin server* tab: If proxy Admin servers are installed in your WCM system in addition to the master Admin server (see section “Managing Proxy Admin Servers” on page 189), you can select the Admin server that the Admin client is to connect to here.
- *View* and *Look and feel* tabs: Here you can change the way items are displayed in the Admin client, e.g. choose a display according to Windows conventions.

Using the Admin Client as a Web Application

You may also use the Admin client without installing it on your local computer. This way, you can manage Livelink WCM Server from different computers. For this purpose, you create a web application for the Admin client and integrate this web application in an application server.

Using the Admin client as a web application makes it possible to significantly reduce the administration effort for the WCM system. Program updates and Service Packs can be installed more easily. Moreover, you do not have to enter the individual installation parameters when installing distributed Admin clients.

Two technologies are available for using the Admin client as a web application: applet and Java Web Start application. The preferred technology should depend on the existing infrastructure in your company. In principle, the Admin client can simultaneously be distributed to different computers both as an applet and as a Java Web Start application.

When using the Admin client as a web application, the following differences exist compared with a local installation:

- No information is written to the log files. All standard output and error output is written to the console of the Java plugin or to the console of Java Web Start.
- The settings for the Admin client, such as information on window size and position, and the configuration options set via *Program* → *Settings* are not stored.
- In the *Tools* menu, the commands *Create web application for Admin client* and *Deploy resources* are not available.

Note: For information on the requirements for using the distributed Admin client, e.g. on the supported operating systems, refer to the Release Notes.

Distributing the Admin Client as an Applet

Applets are Java programs that are downloaded by the web server and executed in the context of the browser. For this type of distribution, a Java plugin is required. When the Admin client is started as an applet, all required program data will be downloaded from the application server when the web application is called. The program data is saved in the cache. The next time the program is started, the system only checks whether the time stamp of the program data has changed. Thus, the program data is updated automatically during each start (e.g. installation of a Service Pack). This presupposes that an application server is running on the respective computer. Without the application server, the applet cannot be started, even if the program code has been downloaded completely.

The Admin server must allow HTTP for the Admin client to be distributed as an applet. To enable HTTP, choose *Configuration* → *Pools* → *WCM* → *{name of the Admin server}* → *WCM connection* tab and click the *HTTP* radio button either for *Preferred connection* or *Alternative connection*.

Distributing the Admin Client as a Java Web Start Application

In contrast to applets, great importance was attached to a quick and comfortable distribution of Java applications during the development of Java Web Start. For version management, cache mechanism, and start options, Java applications provide better solutions than applets.

When the Admin client is started as a Java Web Start application, all required program data is downloaded from the application server. After the first start of the Admin client, no running application server is required, as the existing program data is used (offline use).

> **Note:** When the Admin client is used offline, the program data cannot be updated automatically. For this reason, we recommend you keep the application server running after a successful installation.

Creating a Web Application for the Admin Client

To create a web application for the Admin client:

1. Choose *Create web application for Admin client* on the *Tools* menu.

   The *Create web application for Admin client* dialog box opens.

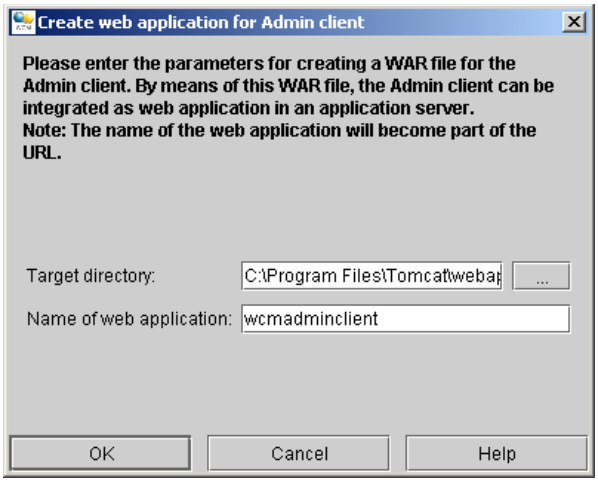

Create web application for Admin client
Please enter the parameters for creating a WAR file for the Admin client. By means of this WAR file, the Admin client can be integrated as web application in an application server.
Note: The name of the web application will become part of the URL.
Target directory:
C:\Program Files\Tomcat\webap
...
Name of web application:
wcmadminclient
OK
Cancel
Help

Fig. 33 – Creating a web application for the Admin client

2. Make the necessary entries for creating the web application. For detailed information on the individual parameters, refer to the Admin client's online help.
3. Click the *OK* button.

After this, add the web application to your application server. The distribution of the Admin client is performed automatically when opening the start page of the web application in the browser (e.g. **http://wcmserver.company.example/wcmadminclient/index.html**). The web application reflects the version level of the Admin client at the time the web application was created.

On the start page of the web application, you can select whether you want to start the Admin client as an applet or as a Java Web Start application.

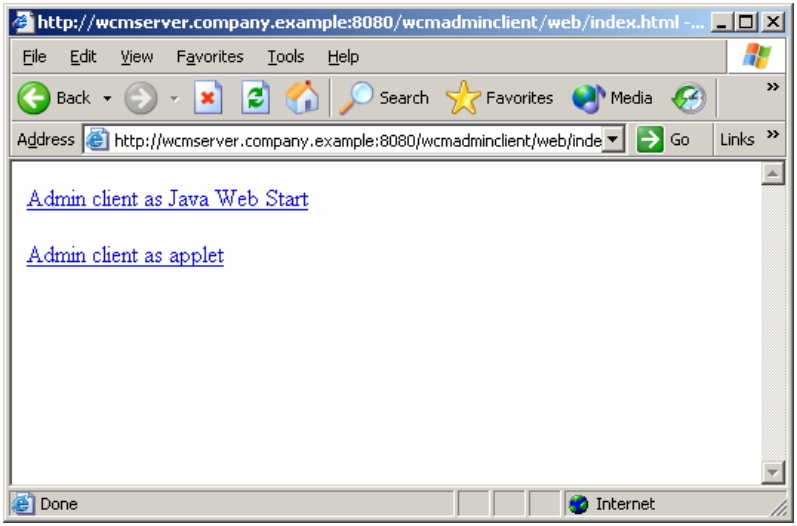


Fig. 34 – Selecting a web application for the Admin client

If you have not yet installed a Java plugin or Java Web Start, it will be installed automatically (only Internet Explorer under Windows). Alternately, you will be forwarded to the respective download page of Sun Microsystems.

Updating the Web Application

If you install a Service Pack or perform an upgrade to a new version of Livelink WCM Server, the web application for the Admin client must also be updated. For this purpose, create a new web application and integrate it in the application server.

If the connection parameters to the Admin server changed, you must modify the file **\{name of the web application}\WEB-INF\web.xml**, which is located in the web application directory of the application server, accordingly. To ensure that the correct connection parameters will be entered the next time the web application is created, also modify the file **web.xml** in the directory **\{WCM installation directory}\admin\web\WEB-INF** on the computer with the locally installed Admin client.

Deploying Resources

By choosing *Deploy resources* on the *Tools* menu, you can deploy local resources to the entire WCM system. These resources include:

- JAR archives
- properties files

  The properties files contain the translated user interface texts for the Admin client, the Content client, and the Content client (Classic). Livelink WCM Server offers the possibility to translate the names of items, such as object types or functional areas. This way, you can, for example, specify an English and a German name for a user-defined object type. This name is then displayed according to the language settings of the users in the clients.

  For further information on translating (localizing) user interface texts, refer to the following section.
- icons for object statuses and object types

To deploy resources:

1. Copy the desired files to the WCM installation directory on the computer hosting your master Admin server.

> **Note:** To deploy the Service Pack files (**vipacs.jar**, **vipapi.jar**, and **vipcore.jar**), copy them to the directory **{WCM installation directory}\latestpatch** on the computer hosting the master Admin server.

2. Choose *Deploy resources* on the *Tools* menu.

   The files are copied from the local WCM installation directory to the respective directories on the computers on which the WCM servers are installed. This also applies to Content servers running as web applications in an application server.

   > **Note:** The files for Search servers and Admin clients will only be updated if these components are installed below the WCM installation directory. If this is not the case, you must copy the changed files manually. This also applies to Admin clients installed separately on computers with no WCM servers.

3. Restart all servers and web applications affected.

Localizing GUI Texts

In the Admin client, you can add custom configuration items, such as functional areas, agents, or connection types. If the users of your WCM system use the clients in different languages, you can localize, i.e. translate, the names of these user-defined items. This way, the translated items are displayed, for example, in a German user interface.

> **Note:** For information regarding translation of the supplied GUI texts of the Livelink WCM Server clients, please contact Gauss Interprise AG.

The localized names of the user-defined items are saved in the so-called properties files, which are located in the following subdirectories of the WCM installation directory:

- **\config\resource**
- **\admin\config\resource**
- **\contentminer\config\resource**

When using an application server, the properties files are also located in the following directories:

- **{WCM installation directory}\admin\web\WEB-INF\classes\config\resource**
- **\{directory of the web application}\WEB-INF\classes\config\resource**

The following table offers an overview of the configuration items that can be localized and of the respective properties files.

Note: The “internal” name in the following table is the name you specify when adding the item.

Table 5 – Configuration items that can be localized

Item	Name of properties file	Format of the entry in properties file

Agents	**ConfigMessage_*.properties**	`&C#AGENT_{internal name}={translated name}`
		Example:
		`&C#AGENT_ExportAgent=WebsiteExport`

Custom connection types	**ConfigMessage_*.properties**	`&C#POOLTYPE_{internal name}={translated name}`
		Example:
		`&C#POOLTYPE_JNDI=LDAP`
		Note: Under *Configuration* → *Custom connection types*, the internal name of the connection type will continue to be displayed. However, when adding a pool which is based on a custom connection type, the localized name is displayed in the selection list.

Repositories	**ConfigMessage_*.properties**	`&C#REPOSITORY_{internal name}={translated name}`
		Example:
		`&C#REPOSITORY_groups=groups`

Applications	**ConfigMessage_*.properties**	`&C#APPLICATION_{internal name}={translated name}`
		Example:
		`&C#APPLICATION_VipHCLApplication=Content client Application`

Item	Name of properties file	Format of the entry in properties file

Functional areas	**FuncAreaMessage_*.properties**	`&FA#{internal name}={translated name}`
		Example:
		`&FA#ADVANCED=Create advanced`

Object types	**ObjectTypeMessage_*.properties**	`{internal name}={translated name}`
		Example:
		`HTML=HTML page`

Attributes and properties	**FieldNameMessage_*.properties**	`{internal name}={translated name}`
		Example:
		`created_by=Author`
		Note: In the Admin client, the internal names of the attributes and properties are displayed, and the localized names are used in the Content client.

E-mails in case of status changes of WCM objects	**MailMessage_*.properties**	`&MM#{internal name}={translated name}`
		Example:
		`&MM#EXPIRED_MAIL_SENT_TO_RECEIVER_{0}=An e-mail with all expired objects was sent to {0}.`

To edit the properties files:

1. In the directory **{WCM installation directory}\config\resource** on the computer of the Admin server, select the properties files you want to change.

   If you want to translate texts for the English user interface, select the respective properties file with the extension **_en.properties**, e.g. **ConfigMessage_en.properties**. The respective German files have the extension **_de.properties**.

2. Add the entries for the user-defined items in the format described to the properties file.

   For example, if you have added a functional area “Images”, add the entry `&FA#Images=Create images` to the file **FuncAreaMessage_en.properties** for the English user interface.

   > **Note:** In the properties files, special characters must be represented as Unicode, e.g. \u00f6 for ö. For further information on Unicode, refer to http://www.unicode.org. For replacing the special characters in the properties files, you can also use the program **native2ascii.exe**, which is located in the directory **\{Java SDK directory}\bin**. Call the program with the following syntax: `native2ascii.exe {name of the source file} > {name of the target file}`.

3. In the Admin client, choose *Deploy resources* on the *Tools* menu.

   The changed properties files from the directory **{WCM installation directory}\config\resource** are distributed to the other local resources directories and the other WCM servers.

Help on the Admin Client

When working in the Admin client, you are assisted by wizards, messages, and an online help.

Wizards

The wizards start automatically when you select a relevant function, such as creating a new website. The wizard guides you through the process step by step.

Online help

The online help of the Admin client is implemented as context-sensitive Java help. The help window for the relevant topic opens, depending on the view or dialog box you are currently working in. You can call the help in various ways:

- with the *Help* button in the right window pane
- with the question mark in the toolbar

- from the context menu

If you choose *Help topics* on the *Help* menu, the start page of the help opens regardless of the current context.

Messages of the Admin client

The Admin client displays message boxes if:

- you attempt to perform actions that are not possible for certain items
- certain actions involve a restart of the client or the server
- changes do not take effect until the next time users log in

Error messages are shown in an information window that contains a *Details* button. Clicking this button displays the detailed error messages of the Java Virtual Machine. Please copy this error information into a file if you intend to contact Technical Support of Gauss Interprise AG.

Errors of the Admin client are also logged in the files **adminclient_out.log** and **adminclient_error.log.tmp**. Both these files are located in the subdirectory **\admin\log** in the WCM installation directory.

> **Note:** You can view the logs of the servers in the *System administration* view (see “Server Logs” on page 329).

CHAPTER 4

User Administration

All users who are to access the WCM system are managed in the Admin client. To group users in accordance with the organizational structure of the company and their tasks and to assign special access rights, you can define groups and roles and assign functional areas.

There are three possible ways to store user information:

- the RDBMS, which is also used for storing the website data
- an LDAP directory service which Livelink WCM Server accesses via the protocol LDAP (Lightweight Directory Access Protocol)

  For information on configuring LDAP integration, refer to the Livelink WCM Server Installation Manual. Use the Admin client to assign the WCM attributes to the principals saved in the LDAP directory server, see section “Setting WCM Attributes in LDAP” on page 134.
- a Livelink user administration

  For information on configuring this integration, refer to the Livelink Integration Manual for the WCM system.

Note on LDAP and Livelink: Users with appropriate administration rights in the WCM system can make changes to users which also affect Livelink and the LDAP directory service. These users do not require any privileges in the Livelink system or LDAP system for this. Users who are allowed to modify principal settings in Livelink or LDAP, do not require administration rights in the WCM system either.

User Administration Functions

To open the user administration, click the

tab in the Admin client. The items you can manage in this view are now displayed in a tree structure.

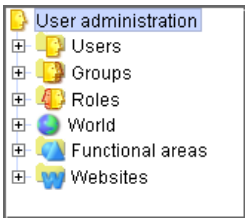


Fig. 35 – User administration items

The following table gives an overview of the functions available for each item.

Table 6 – Items and functions of the user administration

Item	Available functions
User	Add and configure users, edit user information Assign users to groups, roles, functional areas, and websites, and assign default object rights and administration rights See section “Managing Users” starting on page 136
Groups	Add and configure groups, edit group information Assign users, functional areas, and websites to groups, and define default object rights and administration rights See section “Managing Groups and Roles” starting on page 143

Item	Available functions
Roles	Add and configure roles, edit role information Assign users, functional areas, and websites to roles, and define default object rights and administration rights See section “Managing Groups and Roles” starting on page 143
World	This entry represents all users of the WCM system. You can assign administration rights to it. See section “Managing the Rights of the Principal “World”” on page 150
Functional areas	Add functional areas and assign users, groups, and roles to functional areas See section “Managing Functional Areas” starting on page 150
Websites	Assign users, groups, and roles to websites See section “Website Assignments” starting on page 156

By using the filter functions of Livelink WCM Server, you can quickly find the right entry, even with a large number of users, groups, and roles. For further information on searching, see section “Using Filter Functions” on page 104.

Setting WCM Attributes in LDAP

If you use an LDAP directory service to manage your company's user data, you can add the WCM attributes to the users, groups, and roles stored in the directory service and thus enable them to access the WCM system.

This function is only available if you have configured the integration of Livelink WCM Server with the LDAP directory service accordingly and if you have specified an LDAP system for user administration when installing the WCM system. For more information, refer to the Livelink WCM Server Installation Manual.

> **Note:** The LDAP users that are assigned WCM attributes must already have a password in LDAP.

Proceed as follows:

1. Select the *User administration* view.
2. Select one of the items *Users*, *Groups*, or *Roles*, depending on which LDAP entries you want to add the WCM attributes to.
3. Choose *Create WCM attributes in LDAP* on the context menu or click the corresponding icon.

   Icon for creating WCM attributes for users

   Icon for creating WCM attributes for groups

   Icon for creating WCM attributes for roles

   This opens a dialog box in which you select the LDAP entries.

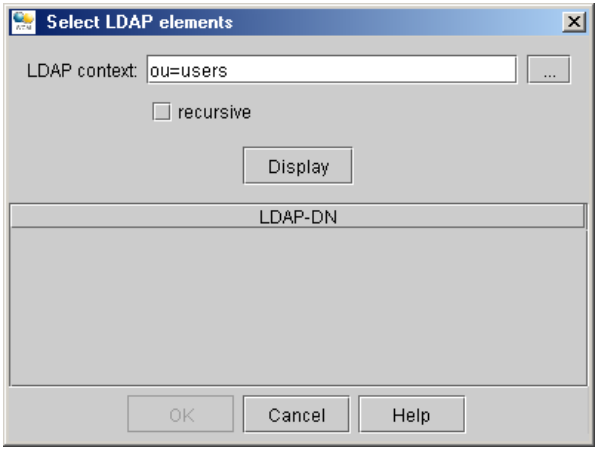


Fig. 36 – Selecting LDAP principals

4. In the *Select LDAP elements* dialog box, enter the LDAP context from which the entries are to be read, or select it by clicking the ... button. If you select the *recursive* check box, the principals of all subordinate name contexts will also be shown.
5. To display the elements of the selected LDAP context, click the *Display* button.

   The LDAP elements are shown in the list with their name (dn = distinguished name).
6. Mark the entries for which you want to enable access to the WCM system.
7. Click the *OK* button.

   The WCM attributes are added to the selected principals. By default, WCM access is activated for the respective users.

Once the WCM attributes have been added, the principals will be displayed in the user administration of the Admin client. You can edit the individual users there and alter WCM settings, such as the e-mail address. The data of the users is modified and saved in LDAP only. The WCM system does not save user data.

Users stored in an LDAP directory service are edited and deleted in exactly the same way as users who are stored in a connected relational database. For notes on the differences between different LDAP directory services, refer to the Livelink WCM Server Installation Manual.

Note: When editing LDAP users in the WCM system, you can only change the user's WCM attributes. Although LDAP-specific settings, such as the position in the LDAP directory tree, are displayed in the Admin client, you cannot change them.

Managing Users

If you expand the main item *Users* in the *User administration* view, a list showing all the users that have access to the WCM system will be displayed. Immediately after installation, the only existing user is the one you set up as WCM administrator during installation.

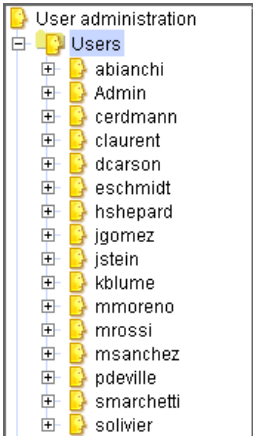


Fig. 37 – Configured users

The following functions are available to you for managing users:

- setting up existing users from your LDAP directory service as WCM users, see “Setting WCM Attributes in LDAP” on page 134
- adding a user, see “Adding a User” on page 138
- editing user information (e.g. e-mail address), see “Editing User Information” on page 139
- editing user assignments, see “Modifying User Assignments” on page 140
- removing a user from the user administration, see “Deleting a User” on page 142

Note: Changes to a user’s settings do not take effect until the user logs in to the WCM system again. As an administrator, you can log out users via the System administration, see section “Managing Logged-in Users” on page 339.

Adding a User

To add a user:

1. Select *User administration* → *Users*.
2. Choose *New user* on the context menu or click the corresponding icon.

   Icon for adding a user

3. In the *New user* dialog box, make the settings for the user.

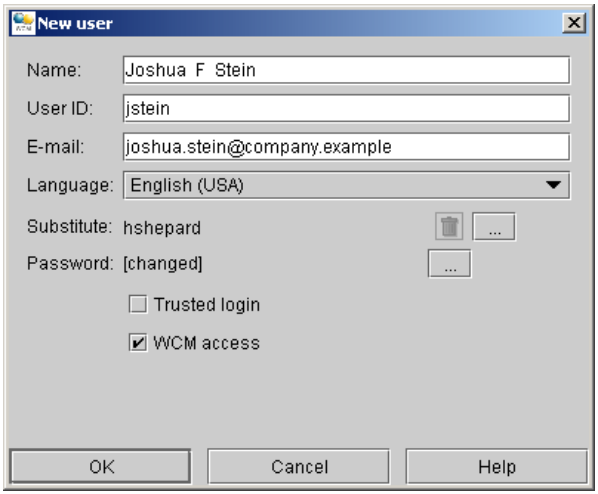


Fig. 38 – Dialog box for adding a user

   For detailed information on the individual fields, refer to the Admin client's online help.

4. Click the *OK* button.

Note for Livelink user administration: The new user is a normal Livelink user with the privileges “Log-in enabled” and “Public Access enabled”. The user is assigned to the Default Group.

Editing User Information

To edit the user information, e.g. the e-mail address:

1. Select *User administration* → *Users*.
2. Mark the desired user in the tree on the left.

   The settings for the user are displayed in the right window pane.

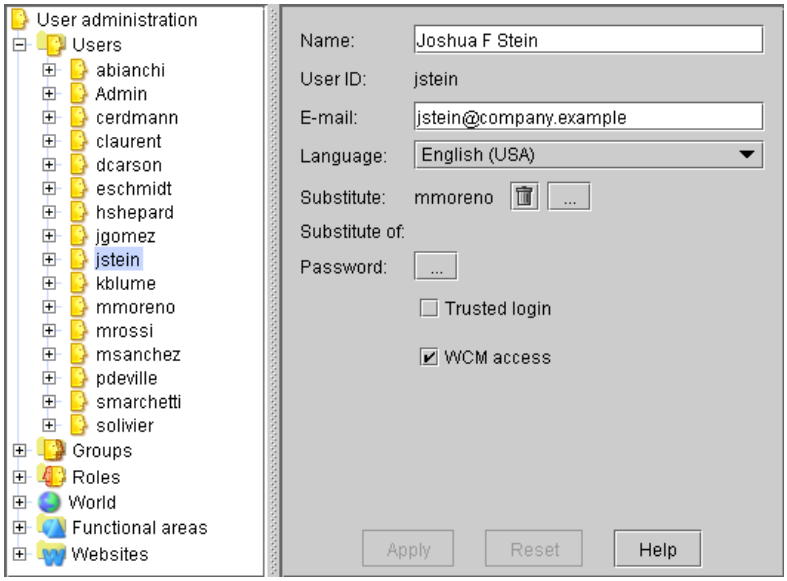


Fig. 39 – Editing user information

3. Make the desired changes.

   For detailed information on the individual fields, refer to the Admin client's online help.

4. Click the *Apply* button.

Modifying User Assignments

By means of the assignments, you can assign a user to a group or role, allow the user access to a website, and determine the user's default object rights and administration rights. For general information on groups, roles, functional areas, and rights, see section "Access Control" starting on page 65.

How to create and remove assignments is described in section "Editing Assignments of Items" on page 109.

To open the assignments of a user, select the respective user via *User administration* → *Users* → *{user ID}* and double-click the user ID. To modify the assignments, use the toolbar or the context menu.

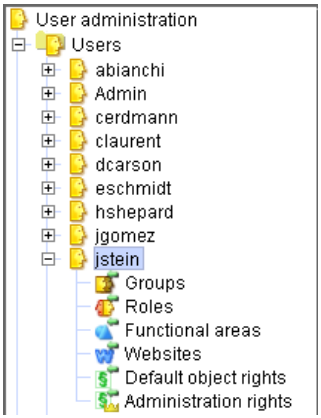


Fig. 40 – Assignments of a user

You can make the following assignments for a user. The overview shows the icons for creating and removing assignments between the items.

Groups: You can assign users to certain groups. Users will receive the rights of the respective group(s).

Roles: You can assign users to certain roles. Users will receive the rights of the respective role(s).

Functional areas: The functional areas are used to determine which types of objects the users may add, check out, and check in, and which dialog boxes and functions are available in the Content client. You can assign functional areas to each user individually.

Websites: If you assign a website to a user, this user can access the objects of this website via the Content client. The exact access rights depend on the user's membership in groups or roles, the user's functional areas, and on the rights settings of the individual WCM objects.

Default object rights: For each user, you can set the default object rights for editing WCM objects. These settings are used as the default access rights when a user is added to the list of persons authorized to access an object in the Content client.

Administration rights: Here you determine the users' rights for the administration of the WCM system. The different rights can be assigned individually. In this way, you can control precisely which settings the individual users can view and what changes they can make. Depending on the assigned rights, the Admin client displays only those views and functions that the user is entitled to use. For example, if the user does not have the right to view the configuration, the Admin client hides this view.

For an overview of all administration rights, refer to table “The individual administration rights” on page 75.

Note: If a user has individual administration rights in addition to the administration rights due to the group or role membership, the rights are added up. Moreover, **all** users have the administration rights of the principal “World”, see section “Managing the Rights of the Principal “World”” starting on page 150.

Deleting a User

To remove a user from the user administration of your WCM system:

1. Select *User administration* → *Users*.
2. Mark the desired user in the tree on the left.
3. Choose *Delete user* on the context menu or click the corresponding icon.

   Icon for deleting a user

4. Confirm the security prompt by clicking the *Yes* button.

The deleted user can no longer log in to the WCM system. If you only want to prevent a user from accessing the WCM system, you can clear the *WCM access* check box in the user’s settings. Thus, you do not need to delete the complete user entry.

Notes

- If you delete a user after you have added it to the access control list of a WCM object in the Content client, the user is not automatically deleted from the list of authorized persons. You must make the necessary changes manually.

- As a result of deleting users, there may be WCM objects that can no longer be accessed by any principal. Choose *Collect orphan objects* on the *Tools* menu to assign such objects to a user.
- A user with administration rights can only be deleted by users that have the right “Change administration rights”.
- If you delete an LDAP user, the corresponding entry will be removed completely from the LDAP directory service.
- If you delete a Livelink user, this user is marked as deleted in Livelink, but not removed from the database.

Managing Groups and Roles

With Livelink WCM Server, you can assign the users of a website to groups and control access to the website objects by assigning rights to these groups. Usually, groups are tied to organizational structures, such as departments or projects, e.g. “Marketing” or “Sales”. Roles offer another way of classifying users. Unlike groups, roles are defined in terms of tasks. e.g. “Project Manager” or “Editor”. For general information on access control by means of groups and roles, see section “Access Control” starting on page 65.

The procedures for managing groups and roles are identical and are therefore described together.

If you open the main item *Groups* or *Roles* in the *User administration* view, the available groups or roles are shown in the tree on the left.

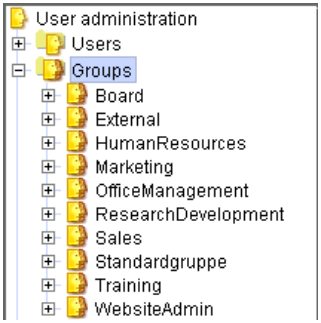


Fig. 41 – Groups of the WCM system

The following functions are available to you for managing groups and roles:

- using existing groups and roles from your LDAP system for the WCM system, see “Setting WCM Attributes in LDAP” on page 134
- adding a group or role, see “Adding a Group or Role” on page 145
- changing the e-mail address or WCM access of a group or role, see “Edit Group or Role Information” on page 146
- editing the assignments of a group or role, see “Modifying the Assignments of a Group or Role” on page 146
- removing a group or role from the user administration, see “Deleting a Group or Role” on page 149

Notes

- Changes to a group or role do not take effect until the assigned users log in to the WCM system again. As an administrator, you can log out users via the System administration, see “Managing Logged-in Users” on page 339.
- Livelink does not differ between groups and roles. For this reason, the WCM roles are represented by Livelink groups. For each Livelink

group, the information is stored whether this group is a group or a role in the WCM system.

- In Livelink, you cannot store additional information, such as the e-mail address, with groups. This means that you have to use the Admin client to edit WCM-specific information of groups and roles.

Adding a Group or Role

To add a group or role:

1. Select *User administration* → *Groups* or *Roles*.
2. Choose *New group* or *New role* on the context menu or click the corresponding icon.

   Icon for adding a group

   Icon for adding a role

3. In the following dialog box, make the settings for the group or role.

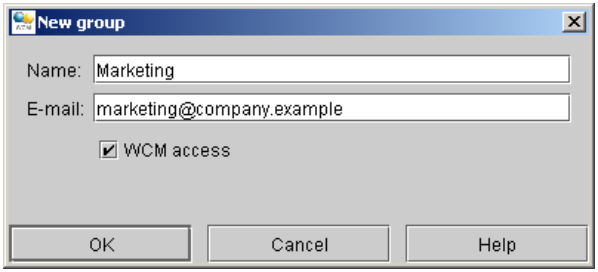


Fig. 42 – Dialog box for adding a group

For detailed information on the individual fields, refer to the Admin client's online help.

4. Click the *OK* button.

Edit Group or Role Information

To change the settings of a group or role:

1. Select *User administration* → *Groups* or *Roles*.
2. Mark the desired group or role in the tree on the left.

   The settings are displayed in the right window pane.
3. Make the desired changes.

   For detailed information on the individual fields, refer to the Admin client's online help.
4. Click the *Apply* button.

Modifying the Assignments of a Group or Role

By means of the assignments, you can assign users to a group or role, allow the group/role access to a website, and set the default object rights and administration rights for the group/role. For general information on groups, roles, functional areas, and rights, see section “Access Control” starting on page 65.

How to create and remove assignments between items is described in section “Editing Assignments of Items” on page 109.

To open the assignments of a group or role, select *User administration* → *Groups* or *Roles* → *{group name/role name}*. Use the toolbar or the context menu to modify the assignments.

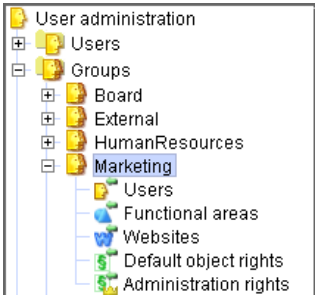


Fig. 43 – Assignments of a group

You can make the following assignments for a group or role. The overview shows the icons for creating and removing assignments between the items.

Users: From the list of stored users, you can select which users are to belong to a certain group or role.

*Functional areas:*The functional areas are used to determine which types of objects the users may add, check out, and check in, and which dialog boxes and functions are available in the Content client. If you assign functional areas to a group or role, all users belonging to this group or role get the respective rights.

Websites: If you assign a group or role to a website, the respective users can access the objects of this website via the Content client. The exact access rights depend on the group and role settings, the assigned functional areas, and the rights settings of the individual WCM objects.

Default object rights: For each group or role, you can set the default object rights for editing WCM objects. These settings are used as default access rights when a group or role is added to the list of persons authorized to access an object in the Content client.

Administration rights: Here you determine the rights of the group or role for the administration of the WCM system. The different rights can be assigned individually. In this way, you can control precisely which settings the assigned users can view and what changes they can make. In accordance with the rights assigned, the Admin client only displays those views and functions that the assigned users are entitled to use. For example, if the group or role does not have the right to view the configuration, this view is hidden in the Admin client.

For an overview of all administration rights, refer to table “The individual administration rights” on page 75.

Note: If a user has individual administration rights in addition to the administration rights due to the group or role membership, the rights are added up. Moreover, **all** users have the administration rights of the principal “World”, see section “Managing the Rights of the Principal “World”” starting on page 150.

Deleting a Group or Role

To remove a group or role from the user administration of your WCM system:

1. Select *User administration* → *Groups* or *Roles*.
2. Mark the desired group or role in the tree on the left.
3. Choose *Delete group* or *Delete role* on the context menu or click the corresponding icon.

   Icon for deleting a group

   Icon for deleting a role

4. Confirm the security prompt by clicking the *Yes* button.

Notes

- If you delete a group or role after you have added it to the list of persons authorized to access a WCM object in the Content client, this change is not adopted automatically. You must update the list of authorized persons manually.
- As the result of deleting groups or roles, there may be WCM objects that can no longer be accessed by any principal. Choose *Collect orphan objects* on the *Tools* menu to assign such objects to a user.
- A group or role with administration rights can only be deleted by users that have the right “Change administration rights”.
- If you delete an LDAP group or role, the corresponding entry will be removed completely from the LDAP directory service.

Managing the Rights of the Principal “World”

The principal “World” represents all users of the WCM system. Technically speaking, it is a group. The administration rights of this principal are valid for all users of the WCM system in addition to the administration rights that have been set for the individual users or the assigned group or role.

Note: By default, all users (i.e. “World”) have only access to the user administration in the Admin client. We recommend that you do not change this in order to reserve access to the configuration and system administration to administrators.

When you modify the administration rights of the principal “World”, you proceed in the same way as for users and groups.

For an overview of all administration rights, refer to table “The individual administration rights” on page 75.

Managing Functional Areas

Functional areas perform two essential tasks:

- They determine which types of objects the users may add, check out, and check in. Some functional areas, such as “Basic”, are by default assigned to object types. Only users that have the corresponding functional area can add, check in, and check out objects of this object type.
- They determine which views and dialog boxes are available to the user in the Content client.

For general information, refer to section “Functional Areas” on page 68.

If you open the main item *Functional areas* in the *User administration* view, a list of available functional areas is displayed.

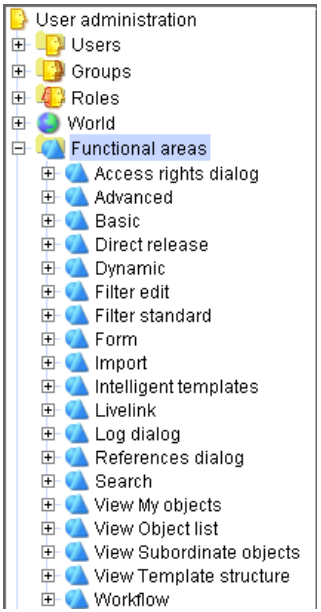


Fig. 44 – Available functional areas

The following functions are available to you:

- adding a custom functional area, see “Adding a Functional Area” on page 152
- viewing the settings of functional areas, see “Settings of Functional Areas” on page 153
- assigning functional areas to users, groups, and roles, see “Assigning Functional Areas” on page 154
- deleting functional areas, see “Deleting a Functional Area” on page 155

Functional areas can also be assigned to object types. This is done in the settings of the object types. By this assignment, you determine that objects with this object type may only be added, checked out, and checked in by users with a certain functional area (*Assignments* tab).

Adding a Functional Area

To add a functional area:

1. Select *User administration* → *Functional areas*.
2. Choose *New functional area* on the context menu or click the corresponding icon.

   Icon for adding a functional area

3. In the following dialog box, enter the name for the new functional area.

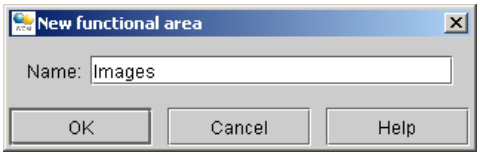


Fig. 45 – Dialog box for adding a functional area

> **Note:** If you want the name of the functional area to be displayed in the language of the user, you can translate it (see section “Localizing GUI Texts” on page 123).

4. Click the *OK* button.

The new functional area will not be available until the Administration server has been restarted. Only then can you assign groups, roles, or individual users to the functional area.

Note: A new functional area must be assigned to a principal to take effect. Moreover, it must be assigned to one or more object types.

Settings of Functional Areas

Note: For displaying the settings of the functional areas, you require the administration right “Access to configuration”.

To view the settings of a functional area, select it via *User administration → Functional areas → {name of the functional area}*. In the right window pane, the name, the website, and the assigned object types are displayed.

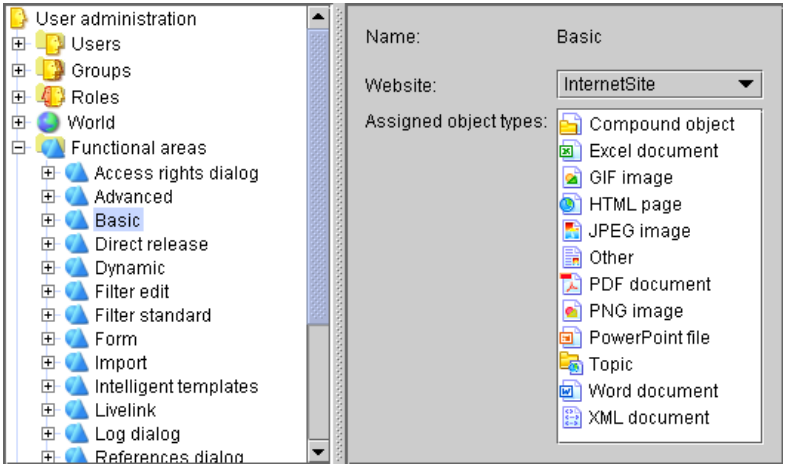


Fig. 46 – Settings of functional areas

In the *Configuration* view, you can change the assignments between object types and functional areas and make further assignments for custom functional areas and object types (see “Object Type Settings” on page 231).

Assigning Functional Areas

If you open one of the functional areas, the list of assignments opens in the tree: *Users*, *Groups*, and *Roles*. If you open one of the assignment items, e.g. *Users*, the right window pane shows a list of assigned items, e.g. the users who are assigned to the functional area “Direct release”.

By means of the toolbar or the context menu, you can make and remove the following assignments:

Assign users and remove assignments

Assign groups and remove assignments

Assign roles and remove assignments

If you assign a user, group, or role to a functional area, the respective users get the rights associated with this functional area (e.g. the right for direct release or the right to add, check out, and check in JSP pages).

If a user is assigned to one functional area due to group or role assignments and to another functional area due to individual assignments, both functional areas apply to the user. That means that the rights are “added up”.

Note: If you modify the functional area assignments, the changes do not take effect until the relevant users log in to the WCM system again. As an administrator, you can log out users via the System administration, see section “Managing Logged-in Users” on page 339.

Deleting a Functional Area

Note: You can only delete custom functional areas that no longer have any users, groups, or roles assigned. Moreover, this functional area must not be assigned to an object type.

To delete a functional area:

1. Select *User administration*→ *Functional areas*.
2. Mark the desired functional area in the tree on the left.
3. Choose *Delete functional area* on the context menu or click the corresponding icon.

Icon for deleting a functional area

Website Assignments

In the *User administration* view, you can use the main item *Websites* to assign users, groups, and roles to websites. To create and configure websites, change to the *Configuration* view of the Admin client (see chapter 7 “Managing Websites”).

Open the main item *Websites* to display the list of assignments to users, groups, and roles.

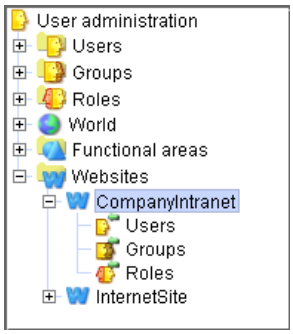


Fig. 47 – Website assignments

By means of the toolbar or the context menu, you can make and remove the following assignments:

Assign users and remove assignments

Assign groups and remove assignments

Assign roles and remove assignments

If you assign a website to a user, group, or role, the respective users can access the objects of this website via the Content client. The exact access rights depend on the users' memberships in groups and roles, the users' functional areas, and on the rights settings of the individual WCM objects.

Note: If you modify the website assignments, the changes do not take effect until the relevant users log in to the WCM system again. As an administrator, you can log out users via the System administration, see section “Managing Logged-in Users” on page 339.

CHAPTER 5

Managing Pools and Connection Types

The entire configuration of your WCM system is performed via the Admin client. To open the configuration, click the Configuration tab in the Admin client.

This chapter describes how to manage pools and custom connection types. For general information on communication and pools, refer to section “Communication Between the Components of a WCM System” starting on page 46.

If you open the tree item *Pools* or *Custom connection types* in the *Configuration* view, all configured pools (sorted by connection types) or all custom connection types will be displayed.

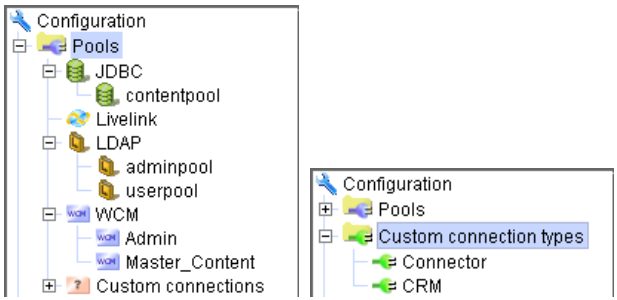


Fig. 48 – Overview of available pools and connection types

Connection types

The connections within the WCM system belong to different types. Depending on the communication partners, the connections have different parameters. Connections between the WCM servers require different parameters than connections to the database, to the LDAP directory service, or to a Livelink system. For this reason, the pools used for managing connections are based on so-called connection types. These connection types provide the required parameters.

During the installation of Livelink WCM Server, the pools required for the WCM system are created automatically. These pools are based on the **default connection types**:

- *JDBC:* connection type for connections to an RDBMS
- *LDAP:* connection type for connections to an LDAP directory service
- *Livelink:* connection type for connections to a Livelink system
- *WCM:* connection type for connections between the WCM servers

You cannot modify or delete the default connection types.

For integrating the WCM system with third-party systems, pools with special connection parameters might be required. To add such pools, you can set up **custom connection types** in the *Configuration* view.

The following functions are available to you for managing custom connection types:

- adding a connection type (see section “Adding a Custom Connection Type” on page 168)
- modifying connection type settings (see section “Connection Types Settings” on page 168)
- deleting a connection type (see section “Deleting a Custom Connection Type” on page 170)

Pools

During the installation of Livelink WCM Server, the required pools are created automatically.

- For communication between the WCM servers: for each server, there is a pool of type “WCM” with the name of the server. These pools are used for connections to the respective server.

  For the connections to a server, the same parameters are used in the entire WCM system by default. For this reason, these pools are also called *global WCM pools*.

- When managing user data in an RDBMS: a JDBC pool for the connection to the database (default name: “userpool”)
- When managing user data in an LDAP directory service: an LDAP pool for the connection to the LDAP server (default name: “userpool”)
- When managing user data in a Livelink system: a Livelink pool for the connection to the Livelink server (default name: “userpool”)

To control the connections within the WCM system, you can configure the existing pools according to your needs and add pools which are based on the default connection types or custom connection types. This way you can, for example, set up special WCM pools for the communication between two WCM servers and integrate several databases, Livelink systems, and LDAP servers.

The following functions are available to you for managing pools:

- adding a pool (see “Adding a Pool” on page 162)
- modifying pool settings (see “Pool Settings” on page 164)
- deleting a pool (see “Deleting a Pool” on page 167). You cannot delete global WCM pools.

Note: A server can only access pools which have been assigned to it. This is done in the assignments of the server, see section “Assigning Pools to Servers” on page 182. Pools which are based on custom connection types cannot be assigned to servers.

Adding a Pool

Pools that you add with the Admin client can be based on one of the default connection types or a custom connection type. New pools are required for different purposes:

- **JDBC pool:** If your user data is managed in an LDAP directory service, no JDBC pool for the connection to an RDBMS is created during installation of Livelink WCM Server. For saving the website data in the database, you must set up a JDBC pool.
- **JDBC pool:** Additional JDBC pools might be required if the WCM servers of a distributed system access separate data storages or if user and website data is to be stored in separate databases.

  Note: When you add a JDBC pool, it must indeed access a different database than the JDBC pools that already exist. Otherwise, problems occur when the new pool is used by the servers.

- **Livelink pool:** If you want to integrate one or more Livelink systems, Livelink pools must be set up. If you WCM system is to access several Livelink systems or several entry points of one Livelink system, you must adapt the parameters in the file **livelink-systems.xml** accordingly. This file is located in the directory **{WCM installation directory}\config**. For information on the individual parameters, refer to the Livelink Integration Manual for the WCM system.

- **LDAP pool:** If you use fallback LDAP servers or if users from different LDAP directory services are to access the same WCM system, additional LDAP pools must be set up.

  Notes

  - Please make sure that only one LDAP pool is set up per LDAP server, i.e. each LDAP pool must access an LDAP server of its own.
  - Please note the information on integrating several LDAP servers in the Livelink WCM Server Installation Manual.
  - If you add an LDAP pool for accessing an LDAP server in order to grant the principals managed by this LDAP server access to the WCM system, the users, groups, and roles of the LDAP directory service must be equipped with the WCM attributes (see “Setting WCM Attributes in LDAP” on page 134).

- **Special WCM pool:** If due to the structure of your network the settings of the global WCM pools cannot be used for the connections between two WCM servers, you can set up so-called *special WCM pools* for the connection between certain servers. If such a pool exists, the respective global WCM pool is not used.

  The settings of a special WCM pool are valid for the connections in one communication direction: from the communication client (which establishes the connection) to the communication server (which accepts the connection). If special settings are also to apply for establishing connections in the opposite direction, you must add a second special WCM pool with exchanged client and server roles.

  The special WCM pool must be assigned to the communication client.

- **User-defined pool:** A new pool on the basis of a custom connection type is, for example, necessary for integrating the WCM system with third-party systems. To add such a pool, you must first set up the respective connection type, see section “Adding a Custom Connection Type” on page 168.

Starting the wizard for new pools

When adding a pool, you are supported by a wizard. To start the wizard:

1. Select *Configuration* → *Pools*.
2. Choose *New pool* on the context menu or click the corresponding icon.

   Icon for adding a pool

3. Follow the instructions given by the wizard that guides you through the installation.

   The individual steps of the wizard are described in more detail in the online help of the Admin client.

Pool Settings

To view or edit the settings of a pool:

1. Select *Configuration* → *Pools* → *{connection type*.
2. Mark the desired pool in the tree on the left.

   In the right window pane, the settings are displayed on various tabs. The type and number of tabs depend on the connection type this pool is based on. The individual parameters are described in detail in the online help of the Admin client.

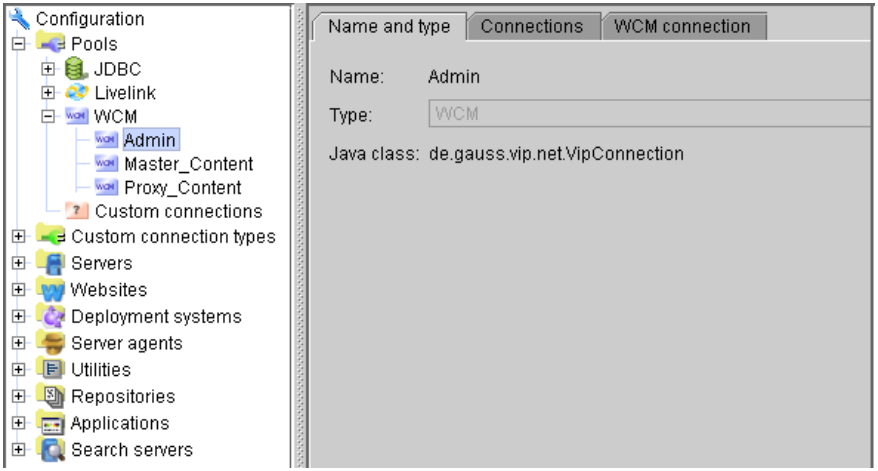


Fig. 49 – Settings of a pool

- You cannot change the entries on the *Name and type* tab. They are defined when the pool is set up.
- On the *Connections* tab, you specify the number of connections that are to be maintained in a pool.
- For JDBC pools: On the *RDBMS parameters* tab, you can change the settings for access to the RDBMS and check the connection from the assigned server(s).
- For Livelink pools: On the *Livelink parameters* tab, you can change the settings for access to the Livelink system and check the connection from the assigned server(s).
- For LDAP pools: On the *LDAP parameters* tab, you can edit the parameters of the LDAP directory service used and check the connection from the assigned server(s).

  On the *LDAP WCM connection* tab, you can change the names of the WCM-specific LDAP object classes.

- For WCM pools: On the *WCM connection* tab, you can change the connection data for the servers. In the extended settings for the protocol VIPP or HTTP, parameters such as buffer sizes, timeouts, or Keep-Alive mechanisms can be defined.
- For user-defined pools: On the *Parameters* tab, you can change the special parameters of pools that are based on a custom connection type.

3. Make the desired changes.
4. Click the *Apply* button.

Notes:

Changed connection data of a WCM server only becomes valid after the respective servers have been restarted.

If you change the host names, SSL settings, or port numbers of an Administration server, the respective entries in the start scripts of the associated servers and of the Admin client must also be modified. The start scripts contain the information for connecting to the Administration server, e.g. `-admin wcmserver.company.com -vipp 5002 -http 5003`.

Deleting a Pool

If a pool is no longer needed, e.g. because the relevant database connection is no longer available, you can delete it. Before deletion, Livelink WCM Server checks whether the pool is no longer used by any server. You can only delete the pool in that case.

Notes:

You cannot delete the global WCM pools which the installation program added for the individual servers.

Before Livelink WCM Server deletes the pool, it creates a backup copy of the directory containing the configuration files. This copy is named **config_YYYY-MM-DD_HH-MM-SS** and is stored in the WCM installation directory. If problems occur after the deletion of the pool, you can replace the configuration files in the directory **{WCM installation directory}\config** with the backup copies. However, changes made to the configuration after the deletion of the pool will be lost.

To delete a pool:

1. Select *Configuration* → *Pools*.
2. Mark the desired pool in the tree on the left.
3. Choose *Delete pool* on the context menu or click the corresponding icon.

   Icon for deleting a pool

4. Confirm the security prompt by clicking the *OK* button.

   If the pool is still assigned to a server, a message is displayed and the operation is aborted.

Adding a Custom Connection Type

When adding a connection type, you are supported by a wizard. To start the wizard:

1. Select *Configuration* → *Custom connection types*.
2. Choose *New connection type* on the context menu or click the corresponding icon.

   Icon for adding a connection type

3. Follow the instructions given by the wizard that guides you through the installation.

   The individual steps of the wizard are described in more detail in the online help of the Admin client.

The new connection type is immediately available for new pools.

Connection Types Settings

To view or edit the settings of a connection type, proceed as follows:

1. Select *Configuration* → *Custom connection types*.
2. Mark the desired connection type in the tree on the left.

   In the right window pane, the settings are displayed on three tabs. The individual parameters are described in detail in the online help of the Admin client.

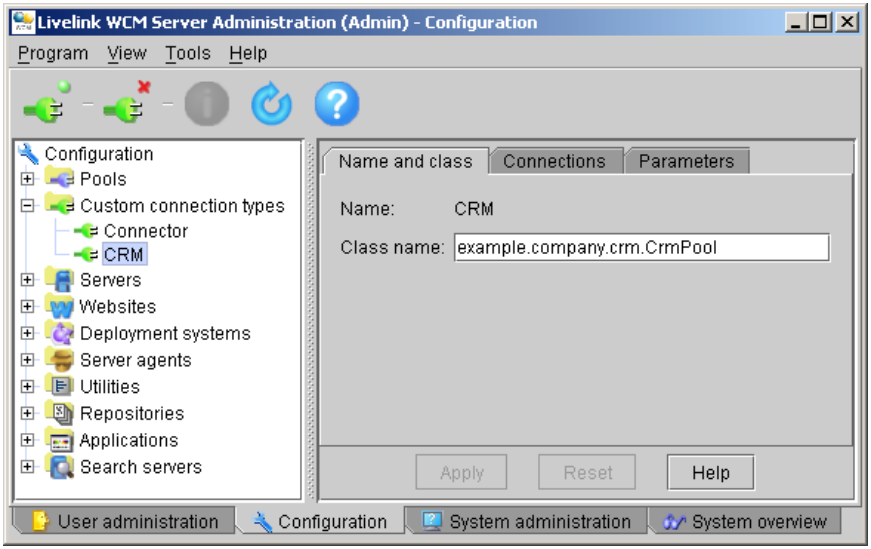


Fig. 50 – Settings of a connection type

- On the *Name and class* tab, you can change the Java class.
- On the *Connections* tab, you specify the default values for the number of connections that are to be managed in the respective pools.
- On the *Parameters* tab, you can edit the special parameters of the connection type.

3. Make the desired changes.
4. Click the *Apply* button.

Note: If you change a connection type, the settings of existing pools which are based on this connection type, are **not** modified automatically. The connection type merely serves as a template for new pools.

Deleting a Custom Connection Type

You can delete connection types that you do not need anymore. Existing pools which are based on this connection type will, however, not be deleted.

To delete a custom connection type:

1. Select *Configuration* → *Custom connection types*.
2. Mark the desired connection type in the tree on the left.
3. Choose *Delete connection type* on the context menu or click the corresponding icon.

   Icon for deleting a connection type

4. Confirm the security prompt.

CHAPTER 6

Managing Servers

The entire configuration of your WCM system is performed via the Admin client. To open the configuration, click the Configuration tab in the Admin client.

This chapter describes how to manage servers. For general information on servers, see section “Basic Components of a WCM System” starting on page 25.

If you open the tree item *Servers* in the *Configuration* view, all installed servers are displayed.

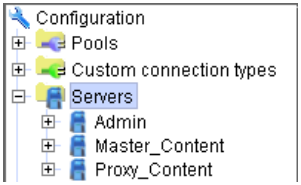


Fig. 51 – Overview of installed servers

The following functions are available for managing servers:

- installing and deinstalling servers

  This is done via the installation program (see Livelink WCM Server Installation Manual).

- editing server settings, see section “General Server Settings” on page 176

- editing assignments of servers. If you open a server, the assignments are displayed in the tree on the left. The following assignments or functions are available.

Table 7 – Server assignments

Assignment	Available functions
Websites	Overview of assigned websites, assign new websites, and remove assignments See section “Websites Assigned to Servers” on page 177
Deployment systems	Overview of the deployment systems installed on this server Add deployment systems See section “Deployment Systems of a Server” on page 180
Pools	Assign pools and remove assignments See section “Assigning Pools to Servers” on page 182
Agents	Assign agents and remove assignments See section “Assigning Agents to Servers” on page 184
Services	Overview of the services that are available on this type of server See section “Services Available on a Server” on page 186

Assignment	Available functions
Secure Access assigned paths	Manage the directories and files for which access is to be controlled by Secure Access See section “Managing Paths for Secure Access” on page 186
Applications	Only for Content servers running in the context of a JSP engine or as a web application in an application server: Assign applications and remove assignments For information on managing applications, see the Portal Manager API documentation.

- registering and managing proxy Admin servers for a distributed WCM system, see section “Managing Proxy Admin Servers” on page 189
- deleting servers from the configuration of the WCM system, see section “Deleting Servers from the Configuration” on page 197

To monitor server activities and change the run level of servers, change to the System administration, see section “Administering Active Servers” starting on page 317.

For information on starting and stopping the servers via the respective start scripts, refer to the Livelink WCM Server Installation Manual.

General Server Settings

To view or edit the settings of a server, proceed as follows:

1. Select *Configuration* → *Servers*.
2. Mark the desired server in the tree on the left.

   In the right window pane, the settings are displayed on various tabs. The available tabs depend on the server type. The individual parameters are described in detail in the online help of the Admin client.

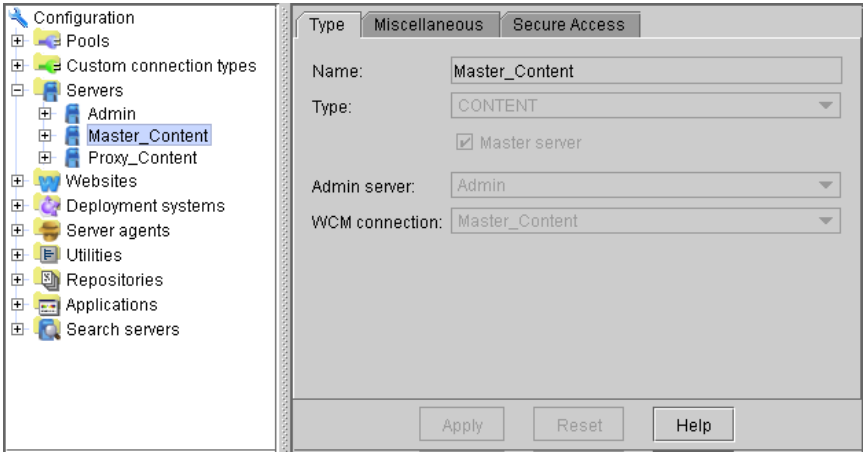


Fig. 52 – Settings of a server

- *Type* tab: The entries on this tab are made during the server installation and cannot be changed.
- *Miscellaneous* tab: On this tab, you can change the e-mail settings, activate support for the remote API, and make settings for the automatic run level check.

- *Administration* tab (only for Administration servers): On this tab, you determine how long the login of users is to remain valid (*Expiration interval*).
- *Secure Access tab:* On this tab, you can switch on the access control component Secure Access for this server, see “Access Control via the Web Server or JSP Engine with Secure Access” on page 78.

  The precise settings and monitored directories are configured via *Configuration → Servers → {server name} → Secure Access assigned paths* (see section “Managing Paths for Secure Access” on page 186).

3. Make the desired changes.
4. Click the *Apply* button.

Websites Assigned to Servers

Select *Configuration → Servers → {server name} → Websites* for an overview of the websites available on this Content server.

Proxy Content servers are usually assigned to a website when the website is created. You can, however, assign servers to websites subsequently, e.g. after adding additional proxy Content servers to your WCM system.

To display a list of the assigned websites in the right window pane, select the item *Websites* in the server’s assignments.

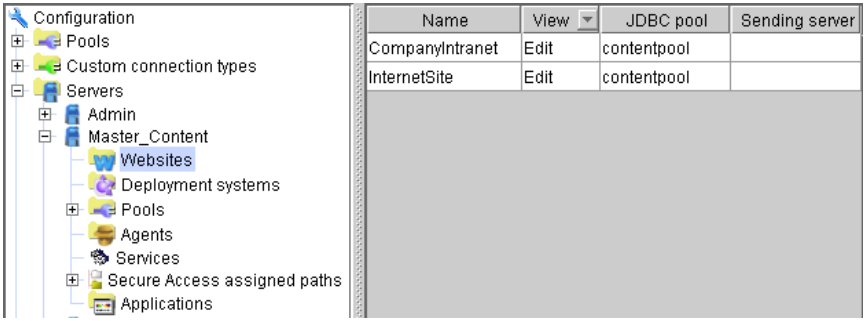


Fig. 53 – Overview of websites assigned to a server

Assigning a Website to a Proxy Content Server

Notes

- If you want to add a proxy Content server, use the installation program of Livelink WCM Server (see Livelink WCM Server Installation Manual).
- If you want to use a separate data storage for a newly assigned proxy Content server, a JDBC pool for accessing this data storage must be set up.
- If you want the proxy Content server to access Livelink objects, assign the corresponding Livelink pool to this server. For information on integrating Livelink systems, refer to the Livelink Integration Manual for the WCM system.
- If the newly assigned proxy Content server is to be used for editing WCM objects by means of the Content client, the proxy Content server must run in the context of a JSP engine or as a web application in an application server.
- Once you have assigned the proxy Content server to a website, you must set up deployment systems for the server so that the pages

generated for the WCM objects are available on the server (see section “Adding a Deployment System” starting on page 275).

Procedure

To assign a website to a proxy Content server:

1. Select *Configuration* → *Servers* → *{server name}* → *Websites*.
2. Choose *Assign website* on the context menu or click the corresponding icon.

   Icon for assigning a website to a proxy Content server

   The *Create assignment between website and server* wizard opens.
3. Follow the instructions of the wizard.

   For detailed information on assigning websites to servers, refer to the online help of the Admin client.

Removing Assignment of a Website to a Proxy Content Server

If the data of a website is no longer to be available on a proxy Content server, you can remove the assignment of the Content server to the website.

Prerequisites

- The website must be in the run level “Website read only”, see “Website Run Levels” on page 341.
- The relevant Content server does not notify any other servers about changes to the website (routing settings), see section “General Website Settings” on page 226.
- The server no longer has any deployment systems for this website.

Procedure

1. Select *Configuration* → *Servers* → *{server name}* → *Websites*.
2. Mark the desired website in the right window pane.
3. Choose *Remove website assignment* on the context menu or click the corresponding icon.

Icon for removing the assignment of a website to a proxy Content server

This server cannot access the website data any longer. You cannot remove the assignment of a master Content server to a website, as this would make it impossible to edit the WCM objects.

Deployment Systems of a Server

The deployment systems generate pages from the WCM objects. These pages can be displayed by means of an HTTP server and a browser. Depending on the type of deployment system installed, the Edit, QA, and/or Production view of the website is generated. For general information on the deployment, refer to section “Deployment” on page 36.

Select *Configuration* → *Servers* → *{server name}* → *Deployment systems* for an overview of the deployment systems installed on this server.

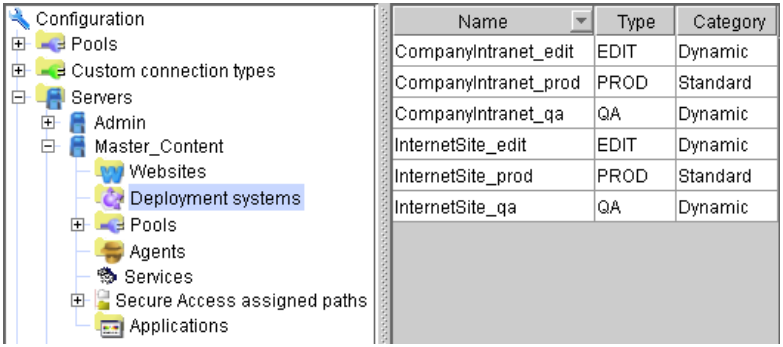


Fig. 54 – Overview of the deployment systems of a server

> **Note:** An overview of installed and available deployment systems of a server is also provided by the DeploymentAdapter report under *System administration → Active servers → {server name} → Reports*.

Deployment systems are set up automatically when websites are created with the options *Minimum* and *Minimum (dynamic)*, and can also be created, configured, and deleted via *Configuration → Deployment systems* (see chapter 8 “Managing Deployment Systems”).

You can also add a deployment system in the server assignments. For this purpose, select the desired server via *Configuration → Servers → {server name} → Deployment systems* and choose *New deployment system* on the context menu. The wizard for adding a deployment system starts (see section “Adding a Deployment System” starting on page 275).

Assigning Pools to Servers

Select *Configuration* → *Servers* → *{server name}* → *Pools* for an overview of the pools used by the selected server.

To actually manage and configure pools, select *Configuration* → *Pools* (see chapter 5 “Managing Pools and Connection Types”).

To display a list of the pools used in the right window pane, open the *Pools* item and the respective connection type (e.g. *WCM*) in the server’s assignments.

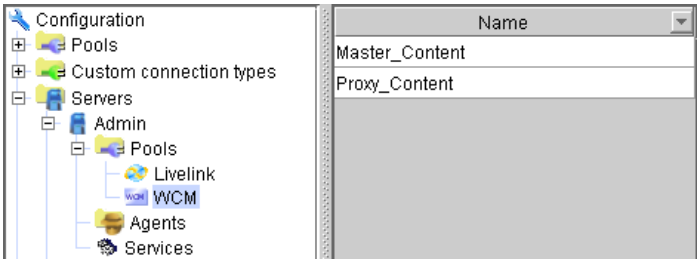


Fig. 55 – Overview of the pools for a server

Note: You create a website in a distributed WCM system in which the proxy Content server for the Production view of the new website is located outside a firewall (outside the corporate network). Please note that in this case the WCM pool of the master Content server is assigned automatically to the proxy Content server when the website is created. If you want to prevent connections through the firewall from this proxy Content server to the master Content server, remove the assignment of this pool.

The following functions are available to you on the context menu or the toolbar:

Assigning a pool to a server (see also “Creating Assignments” on page 109)

Thus, the server can use this pool for saving website data or for notifying other servers. Pools which are based on custom connection types cannot be assigned to servers.

Removing the assignment of a pool to a server (see also “Removing Assignments” on page 112)

The server type determines which connection types you may assign. In the *Select pools* dialog box, only those pools that can be assigned to the respective server are displayed. For example, if you use an LDAP-based user administration, you can only assign LDAP pools to the Admin server; you cannot assign JDBC pools. LDAP pools cannot be assigned to Content servers as JDBC pools are always used for storing website data. When assigning several LDAP pools to a server (e.g. for integrating fall-back LDAP servers), you can determine the sequence of the LDAP pools (see the following section

Determining the Sequence of the LDAP Pools

If you have assigned the Admin server multiple LDAP pools, e.g. for using a fallback LDAP server or several LDAP servers (see Livelink WCM Server Installation Manual), you can determine which LDAP server the Admin server is to connect to first.

Select *Configuration* → *Servers* → *{name of the Administration server}* → *Pools* → *LDAP* to display an overview of the LDAP pools assigned to the server.

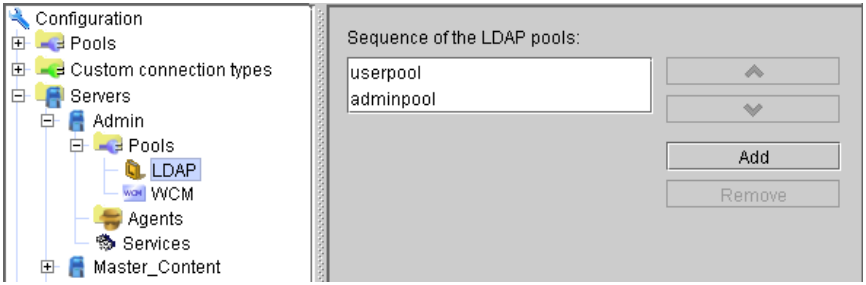


Fig. 56 – Determining the sequence of the LDAP pools

If the first pool in the list is not available, the other pools will be contacted in the sequence you specified. Use the buttons and to change the sequence of the LDAP pools.

Assigning Agents to Servers

Server agents are Java programs that are loaded when a server starts. Server agents run in the same runtime environment of the Java Virtual Machine (JVM) as the relevant server. Agents perform special functions and can be used to automate processes in the WCM system. For this purpose, they use the WCM Java API of Livelink WCM Server (see WCM Java API Programmer's Manual).

A number of standard agents are supplied with Livelink WCM Server. Some of these agents are automatically installed and assigned to servers when setting up a WCM system or a website. Other agents supplied have to be manually integrated in the WCM system and assigned to a server in order to become active. Similarly, if you develop new agents on the basis of the WCM Java API, you must first integrate them and then assign them to a server.

Agents are integrated and deleted under *Configuration* → *Server agents*, see section "Managing Server Agents" starting on page 282.

In the server assignments (*Configuration → Servers → {server name} → Agents*), you can see an overview of the agents assigned to the server. All assigned agents are started automatically when the server starts or changes from run level 3 to run level 4.

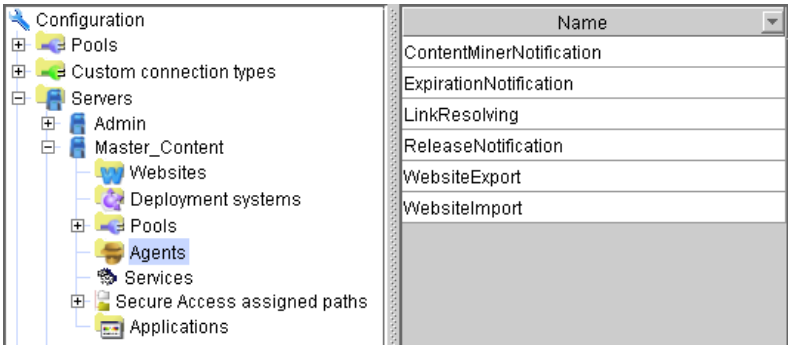


Fig. 57 – Overview of the agents of a server

The following functions are available to you on the context menu or the toolbar:

Assigning an agent to a server (see “Creating Assignments” on page 109)

Removing the assignment of an agent to a server (see also “Removing Assignments” on page 112)

For an overview of the status of the agents assigned to a server, select *System administration → Active servers → {server name} → Agents*. Here you can start and stop the agents individually and regardless of the server run level. See “Assigned Agents” on page 335.

Services Available on a Server

Select *Configuration* → *Servers* → *{server name}* → *Services* for a list of the services available on the selected server. These services may be used indirectly by means of the functions of the WCM Java API. In the Admin client, the services are displayed, but cannot be added, changed, or deleted.

Managing Paths for Secure Access

The deployment systems of a Content server generate HTML files, JSP pages, etc. from the WCM objects and store these files in the configured directories. These directories can be accessed via an HTTP server and a web browser. In order to protect the generated files from unauthorized access, e.g. via the Internet, you can arrange for certain directories or all directories in a deployment system to be monitored by Secure Access.

For general information on Secure Access, refer to section“Access Control via the Web Server or JSP Engine with Secure Access” on page 78. For information on configuring web servers for Secure Access, refer to the Livelink WCM Server Installation Manual.

If an attempt is made to access files in monitored directories, Secure Access checks whether access authorization is necessary for the page requested. In this case, the user must provide authentication for access to the page.

Before you can set paths for Secure Access in the server assignments, you must activate access control by Secure Access. This is done in the server settings on the *Secure Access* tab.

Select *Configuration* → *Servers* → *{server name}* → *Secure Access assigned paths* to enter the directories of a deployment system that are to be protected. If you specify a path here, all directories below that path are

monitored by Secure Access. You can exclude individual directories within this protected path from the monitoring by defining these directories as a path for Secure Access and explicitly deactivating the monitoring.

Notes:

For a better overview, it is advisable to have Secure Access monitor complete paths, including all subdirectories. Your website data should be structured accordingly.

The configuration of the Secure Access paths must correspond to the web server settings.

Select *Secure Access assigned paths* to display the monitored directories which are already configured. The directories are shown in the right window pane and in the tree on the left.

Adding and Editing Paths for Secure Access

To add a path for Secure Access:

1. Select *Configuration* → *Servers* → *{server name}* → *Secure Access assigned paths*.
2. Choose *New path for Secure Access* on the context menu or click the corresponding icon.

   Icon for adding a path for Secure Access

   To edit an existing path, select it via *Secure Access assigned paths* → *{path name}*.

   The settings are displayed in the right window pane.

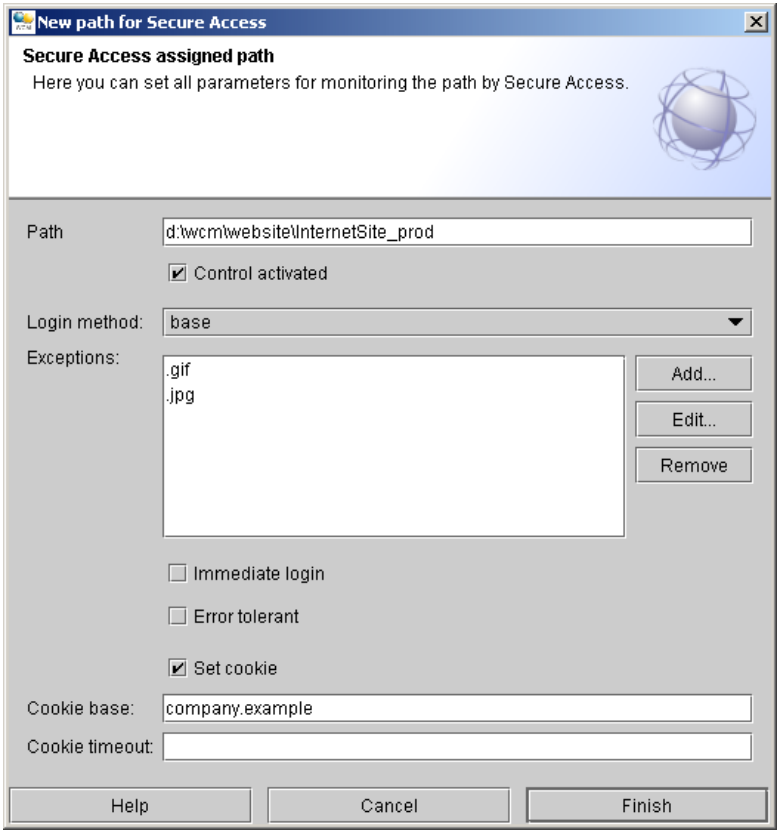


Fig. 58 – Settings of a path for Secure Access

For detailed information on the individual fields, refer to the Admin client's online help.

3. Click the *Finish* or *Apply* button.

Note: After adding new paths to the configuration of Secure Access, the web server must be restarted so that it can read the new Secure Access configuration.

Removing a Path from Secure Access

To remove a directory from being monitored by Secure Access:

1. Select *Configuration* → *Servers* → *{server name}* → *Secure Access assigned paths*.
2. Mark the desired path in the tree on the left.
3. Choose *Delete path setting for Secure Access* on the context menu or click the corresponding icon.

Icon for deleting a Secure Access path setting

Managing Proxy Admin Servers

You require a proxy Admin server if you:

- use a WCM system distributed over a WAN
- set up a proxy Content server for the Production view outside a firewall. The structure of a WCM system with firewall is described in section “Distributed System with Firewall” on page 57.
- want to use a second Admin server in addition to the master Admin server

The associated proxy Content servers contact the proxy Admin server instead of the master Admin server. The proxy Admin server has the following tasks:

- loading server configuration at startup
- logging in users
- checking licenses

First, you install the proxy Admin server and the associated Content servers by means of the installation program. After this, you must register the proxy Admin server in the configuration of the master Admin server, so that the proxy Admin server is notified of any configuration changes and receives the modified data. You can register as many proxy Admin servers as you wish.

Notes

- The Content servers, which are assigned to the proxy Admin server, must have unique names which are not used in the master system.
- Master and proxy Admin servers should access the same user administration, i.e. the same LDAP server, the same Livelink server, or the same database. For user administrations based on LDAP or an RDBMS, you can use separate servers provided that the user information is kept identical by means of synchronization between the servers. This synchronization does **not** belong to the tasks of the WCM system. The Admin servers must access the same type of user administration, e.g. both a database. You cannot mix different user administration types.
- The initial administrator of the proxy WCM system must have **the same** user ID as the administrator of the master WCM system.

Changing the WCM system configuration

Via the master Admin server: After registering a proxy Admin server, the configuration of the WCM system can by default only be changed via the master Admin server. The master Admin server transfers the changes to all registered proxy Admin servers.

If the WCM system configuration was changed and the master Admin server cannot access a proxy Admin server, the master server will try to transfer the changed configuration at defined intervals. If this is not possible, the configuration is synchronized automatically the next time the proxy Admin server is accessed. Information on the transmission attempts

is contained in the ConfigurationManager report, which can be opened via *System administration → Active servers → {server name} → Reports*.

Via proxy Admin servers: If you do not use the proxy Admin server in a firewall scenario, but as a second Admin server, you can allow configuration changes to be made via the proxy Admin server. To do so, assign the pool of the master Admin server to the proxy Admin server, see section “Assigning Pools to Servers” on page 182. This proxy Admin server is now able to transfer changes made via a connected Admin client to the master Admin server.

The following functions are **not** available for an Admin client connected to a proxy Admin server:

- synchronizing configuration
- deregistering proxy Admin servers
- deploying resources

Functions for proxy Admin servers

The following functions are available for proxy Admin servers:

- registering proxy Admin servers, see “Registering a Proxy Admin Server” on page 192
- synchronizing the configuration of master and proxy Admin servers after setting up additional Content or Search servers in the proxy system, see “Synchronizing Configuration Data of Master and Proxy Admin Servers” on page 194
- deregistering proxy Admin servers, see “Deregistering a Proxy Admin Server” on page 195

Registering a Proxy Admin Server

First, you install the proxy Admin server and the associated Content servers by means of the installation program

After this, you register the proxy Admin server in the configuration of the master Admin server.

1. Start the master and proxy Admin servers.
2. Start the Admin client for the WCM system in which the master Admin server is located.
3. Select the master Admin server by via *Configuration* → *Servers* → *{server name}*.
4. Choose *Register proxy Admin server* on the context menu or click the corresponding icon.

   Icon for registering a proxy Admin server

   This opens the *Register proxy Admin server* dialog box.

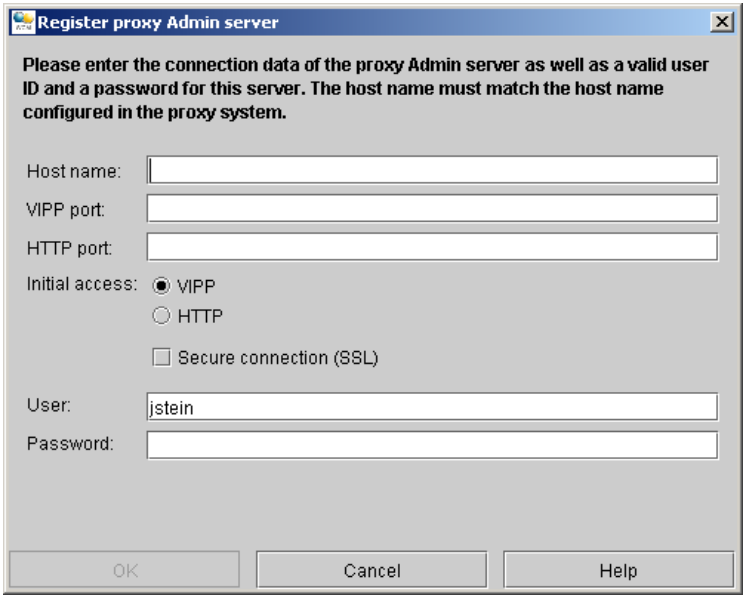


Fig. 59 – Registering a proxy Admin server

5. Enter the connection data of the proxy Admin server. These entries must be identical to the configuration of the proxy system.

   Moreover, a user name and password are required for accessing the proxy Admin server. The user specified must at least have the administration right “Create, modify, delete configuration entry” for the proxy system.

6. Confirm the settings by clicking the *OK* button.

All Content and Search servers that were managed by the proxy Admin server are added to the overall system. The proxy Admin server transmits the information on the relevant pools and servers to the master Admin server, which adds the data to its configuration.

The configuration files of the master Admin server are then copied to the file system of the proxy Admin server. This ensures that the same configuration information is available on both Admin servers.

The users that have administration rights for the master system get these rights for the overall system. After registering the proxy Admin server, the administration rights of these users are valid for both the master and the proxy system. The users, who originally had administration rights for the proxy system, loose these rights. If you deregister the proxy Admin server, these users will get the administration rights back.

Synchronizing Configuration Data of Master and Proxy Admin Servers

All configuration changes in the overall system are made on the master Admin server, which forwards them to the proxy Admin server. This automatically synchronizes the configuration data in the direction master → proxy. However, if you add further Content or Search servers in the proxy system or remove servers, the master Admin server must be notified about this change manually by means of the function *Synchronize configuration*.

Notes:

No configuration changes must be made in the master system while new servers are being installed in the proxy system. Otherwise, the settings of the new servers in the proxy system would be overwritten when the configuration changes are automatically transferred by the master Admin server. To ensure that the configuration cannot be changed by other users, you can set the servers of the master system to run level 4 “Single user mode” (see “Server Run Levels” on page 318).

For synchronizing the configuration after the installation of new servers in the proxy system, only the two Admin servers need to be running.

To synchronize the configuration of proxy and master Admin server:

1. Make sure that the Admin client is connected to the master Admin server of the WCM system (see section “General Server Settings” on page 176).
2. Select the proxy Admin server via *Configuration* → *Servers* → *{server name}*.
3. Choose *Synchronize configuration* on the context menu or click the corresponding icon.

Icon for synchronizing the configuration between proxy and master Admin servers

The proxy Admin server's configuration data on servers and pools is synchronized with the configuration data for the overall system. This adds new pools and servers to the configuration and removes deleted servers or pools from the configuration.

Deregistering a Proxy Admin Server

You can remove a proxy Admin server from the overall system at any time, e.g. if you want to assign it to a different master Admin server or if the structure of your WCM system changes.

This presupposes that the servers of the proxy system are no longer assigned any websites that are also managed in the master system. For this reason, you must remove the relevant assignments before deregistering the proxy Admin server, see “Removing Assignment of a Website to a Proxy Content Server” on page 179.

Note: If the proxy Admin server is damaged or inaccessible, the assignments of the servers cannot be removed. In this case, the proxy Admin server cannot be deregistered. Use the function *Delete server* to remove such a useless proxy Admin server from the configuration of the WCM system (see section “Deleting Servers from the Configuration” on page 197). In contrast to a regular deregistration, the proxy system can no longer be registered with another master system.

To remove a proxy Admin server from the overall system:

1. Make sure that the Admin client is connected to the master Admin server of the WCM system (see section “General Server Settings” on page 176).
2. Select the proxy Admin server via *Configuration* → *Servers* → *{server name}*.
3. Choose *Deregister proxy Admin server* on the context menu or click the corresponding icon.

Icon for deregistering a proxy Admin server

The configuration data of the Content and Search servers and the configuration data of the proxy system's pools is removed from the configuration of the master Admin server. Similarly, the configuration data of the master system is removed from the configuration of the proxy Admin server. This means that only the configuration of the proxy system is left on the proxy Admin server.

The users, who had administration rights for the proxy system before the proxy Admin server was registered, get these rights back. That means that users, who only have administration rights for the master system, cannot access the proxy system any longer.

Note: After deregistration, the proxy system only has a proxy Admin server. As a result, no websites can be created and managed in this system. To be able to use the proxy system again, you must assign it to a new master Admin server.

Deleting Servers from the Configuration

If a server is no longer needed, you can remove it from the WCM system. By default, this is not done via the Admin client, but via the installation program (see Livelink WCM Server Installation Manual).

You can only deinstall servers that are not assigned to any website. For this reason, the respective assignments must be removed via the Admin client before the server can be deleted via the installation program.

If a server is damaged or inaccessible for other reasons, it is possible that it cannot be deleted via the installation program because the assignments of the server cannot be removed.

For such a case, the *Configuration* view provides the function *Delete server* for removing a server from the configuration of the WCM system. Thus, the license used by the server becomes available again.

This function is not available for the master Content server and the master Admin server because the WCM system would no longer be functional after the deletion of these servers.

Important! You should only use the function *Delete server* if it is not possible to delete the server via the installation program and if the correct functioning of the WCM system is affected by this server. Please contact the Technical Support of Gauss Interprise AG before using this function.

Notes on deleting a server

The following actions are performed when a server is deleted:

- The entries of the server are deleted from the configuration files of the WCM system. The files of the server and all entries in the connected database will not be removed.
- The deployment systems of the server are deleted.
- If the server is part of the notification chain of a website (routing settings of the website), it is removed from the chain. Afterwards, the system tries to close the chain in order to prevent communication gaps.
- The global WCM pool of the server is deleted and removed from the assignments of the other servers. All assignments containing this pool are removed.
- All assignments containing this server are removed.

Backup copy of the configuration files

Before the server information is deleted from the configuration files, a backup copy of the directory **{WCM installation directory}\config** is created. The copied directory has the name **config_YYYY-MM-DD_HH-MM-SS**.

When a server is deleted, only the configuration files are modified, but no changes are made in the database. Thus, you can use the backup copy to restore the state before the deletion of the server. For this purpose, copy the files from the backup **config** directory to the directory **{WCM installation directory}\config**. All changes to the configuration that you performed after deleting the server will be lost.

> **Note:** After overwriting the configuration files, all servers must be restarted so that the configuration data can be read.

Performing the deletion of a server

To delete a server from the configuration of the WCM system:

1. Select *Configuration→ Servers*.
2. Mark the desired server in the tree on the left.
3. Choose *Delete server* on the context menu or click the corresponding icon.

   Icon for deleting a server from the configuration

   A dialog box with notes on deleting the server opens. Please read these notes carefully.
4. If you want to delete the server, click the *Yes* button. To cancel the operation, click the *No* button.

   After the confirmation, the assignments of the selected server are analyzed. The next dialog box displays a summary of the actions that will be performed during the deletion of the server:

   - names of the websites for which the routing must be changed
   - names of the deployment systems that will be removed
5. If you want to delete the server, click the *Yes* button again. To cancel the operation, click the *No* button.

   After the confirmation, the selected server is removed from the configuration of the WCM system and the actions described above are performed.

CHAPTER 7

Managing Websites

The entire configuration of your WCM system is performed via the Admin client. To open the configuration, click the Configuration tab in the Admin client.

This chapter describes how to manage websites. You can set up several websites in your WCM system. Each website is managed by exactly one master Content server. The website data may also be available on several proxy Content servers. For general information on the structure of a WCM system, refer to section “Scenarios for Setting up a WCM System” starting on page 55.

If you open the tree item *Websites* in the *Configuration* view, all websites managed in the WCM system are displayed.

Fig. 60 – Overview of managed websites

The following functions are available for websites:

- creating new websites, see section “Creating a New Website” starting on page 204
- editing website settings (see section “General Website Settings” on page 226)

- editing assignments of websites. Double-click the website item to open the list of assignments.

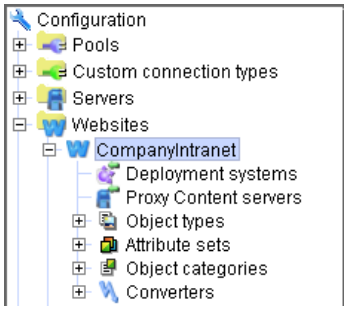


Fig. 61 – Assignments of a website

The following table provides an overview of the functions that are available for these assignments.

Table 8 – Assignments of websites

Assignment	Available functions
Deployment systems	Overview of the deployment systems that are assigned to the website; adding deployment systems See section “Deployment Systems of a Website” on page 227
Proxy Content servers	Overview of the proxy Content servers on which the website is available, assign additional proxy Content servers to a website, and remove assignments See section “Proxy Content Servers Assigned to a Website” on page 228

Assignment	Available functions
Object types	Add, edit, and delete object types, e.g. “HTML page” or “CGI script”. Object types are managed separately for each website. See section “Managing Object Types of Websites” on page 229
Attribute sets	Add, edit, and delete attribute sets which are used to define object types. Like object types, attribute sets are website-specific. See section “Managing Attribute Sets of Websites” on page 234
Object categories	Add, edit, and delete object categories, e.g. “Invoice”. Object categories are managed separately for each website. See section “Managing Object Categories of Websites” on page 237
Converters	Manage conversion programs See section “Assigning Converters to Websites” on page 240

- finding orphan objects of a website and assigning them to a user. WCM objects are considered as orphan if no valid principal (group, role, or user) is entered in their access control list as authorized to access the object. Such objects can no longer be accessed with the Content client. See section “Reassigning Orphan Objects” on page 243.
- exporting and importing websites, see section “Exporting and Importing Websites” starting on page 246

Creating a New Website

Please note the following points before you start configuring a new website:

- If the new website is to be managed by different Content servers than those already set up, you must use the installation program to add the desired servers before you create the website. For information on adding servers, refer to the Livelink WCM Server Installation Manual.
- All Content servers on which the website is to be available later must be active and accessible.
- If the servers are to access database connections for which no pool has yet been set up in your WCM system, you can create such a pool while installing the website. This is always necessary if – when installing the WCM system – you specified an LDAP directory server or a Livelink system for storing the user data. In that case, no JDBC pool is created during installation of Livelink WCM Server. Even if an RDBMS is used for storing the user data, a new JDBC pool is required if website and user data is to be saved in different databases.
- If you create a website in a distributed WCM system, in which, for example, the proxy Content server for the Production view of the new website is located outside a firewall (outside the corporate network), note that when creating the website, the WCM pool of the master Content server is automatically assigned to the proxy Content server. If you want to prevent connections through the firewall from the proxy Content server to the master Content server, remove the assignment of this pool via *Configuration* → *Servers* → *{name of the proxy Content server}* → *Pools*.

Starting the Wizard

A wizard helps you create the new website. Proceed as follows:

1. Select *Configuration* → *Websites*.
2. Choose *New website* on the context menu or click the corresponding icon.

   Icon for creating a new website

3. Specify the configuration of the new website.

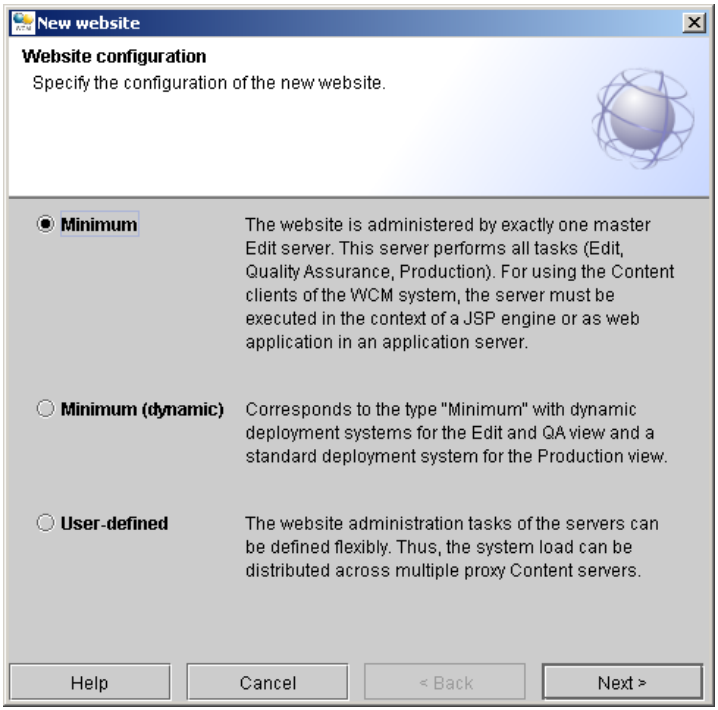

New website
Website configuration
Specify the configuration of the new website.
Minimum
The website is administered by exactly one master Edit server. This server performs all tasks (Edit, Quality Assurance, Production). For using the Content clients of the WCM system, the server must be executed in the context of a JSP engine or as web application in an application server.
Minimum (dynamic)
Corresponds to the type "Minimum" with dynamic deployment systems for the Edit and QA view and a standard deployment system for the Production view.
User-defined
The website administration tasks of the servers can be defined flexibly. Thus, the system load can be distributed across multiple proxy Content servers.
Help
Cancel
< Back
Next >

Fig. 62 – Options when creating a new website

- *Minimum:* The website is managed on exactly one master Content server, on which three standard deployment systems – one for Edit, QA, and Production each – are installed. For general information, refer to section “Minimum System” on page 56.

  See “Creating a Website with the Option Minimum or Minimum (dynamic)” starting on page 207

- *Minimum (dynamic):* The website is installed on a master Content server. The master Content server has dynamic deployment systems for the Edit and QA views and a standard deployment system for the Production view.

  See “Creating a Website with the Option Minimum or Minimum (dynamic)” starting on page 207

- *User-defined:* In this type of installation, you individually determine the parameters for the website, such as assignments of proxy Content servers or deployment systems.

  See “Creating a Website with the Option User-defined” starting on page 218

Note: Livelink WCM Server automatically checks whether enough Content servers and licenses for deployment systems are available for the different options. If this is not the case, the respective options are dimmed and the wizard indicates the reason.

Creating a Website with the Option *Minimum* or *Minimum (dynamic)*

Select the desired option in the first dialog box of the new-website wizard: *Minimum* or *Minimum (dynamic)*.

Step 1 – Specify Website Name and JDBC Pool

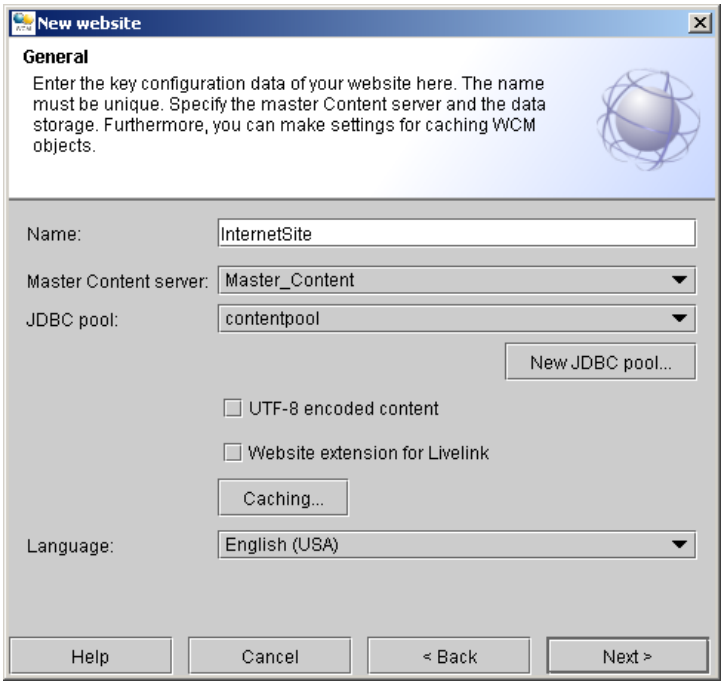


Fig. 63 – Basic information for the new website

- *Name:* Enter the name of your website, e.g. “InternetSite”.
- *Master Content server:* Select the Content server that is to be used as the master server for this website. Only this server has write access to the WCM objects.

> **Note:** The master Content server must run in the context of a JSP engine or as a web application in an application server. This is required for using the Content client, the Content client (Classic), and the Portal Manager API.

- *JDBC pool:* Specify the JDBC pool for the database connection that the master Content server is to use for storing the WCM objects. If the WCM objects are to be stored using a database connection that already exists, select the appropriate pool from the list. If a new database connection is to be used for storing the objects, you can click the *New JDBC pool* button to add a pool. This starts the wizard for adding pools (see section “Adding a Pool” on page 162). The relevant RDBMS must be installed and accessible.
- *UTF-8 encoded content:* If characters that are not contained in the character set Latin-1 (ISO 8859-1) are used in the content and metadata of the WCM objects, you can select this check box to set the website to UTF-8 encoding, i.e. Unicode. This might, for example, be necessary for supporting Asian languages.

  If you select this check box, the following tag is inserted in the head element of the HTML page when the page is generated: `<meta http-equiv="content-type" content="text/html; charset=UTF-8">`. When the WCM tags in the page content are replaced, the characters will be UTF-8-encoded.

  Only select this check box if you require Unicode support. For Western European languages, the Latin-1 character set is sufficient. The content of the pages must also be UTF-8 encoded, i.e. editor programs supporting Unicode must be used for creating and editing the object content.

> **Note:** The use of UTF-8 must be configured consistently for all components of the WCM system, i.e. for the database, the website, and the web server. Please note the general information on using Unicode with Livelink WCM Server in section “Unicode with Livelink WCM Server” on page 82.

- *Website extension for Livelink:* Select this check box if you want to use objects from a Livelink system in your website. The required configuration changes in the WCM system will be made automatically. Also, the database table will be extended so that references to Livelink objects can be stored.
- *Caching:* Click the *Caching* button to set the parameters for caching WCM objects. WCM objects can be loaded from the database into the cache to speed up access to the objects. The minimum cache size should be greater than or equal to the number of website objects.

  After the website has been created, you can still modify the cache settings to suit your requirements, see section “General Website Settings” on page 226.
- *Language:* Select a language for the root object, which is automatically generated during creation of the new website. This setting is written to the metadata of the root object.

Confirm your settings by clicking the *Next* button.

Step 2 – Assign a User, Group, or Role

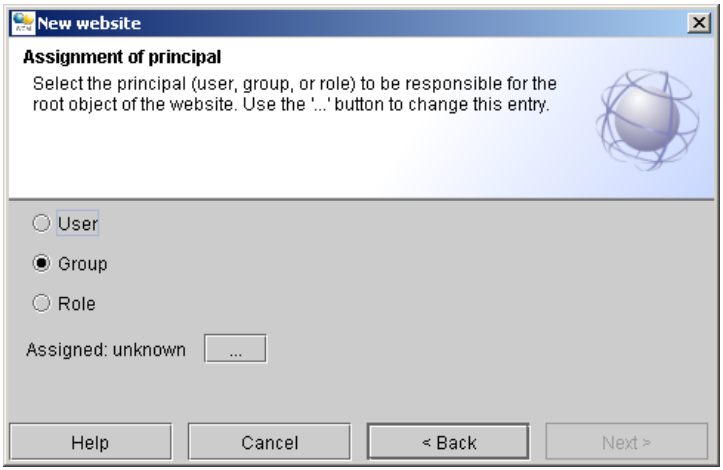


Fig. 64 – Initial assignment of a principal to a website

In this dialog box, you can initially assign *one* principal (user, group, or role) to the website. The assigned principal has unlimited access to the root object of the new website, i.e. the principal can add, change, and release topics on the first level of the website, and assign access rights for these topics. You should select a group or role here to grant several users access to the root object.

To select a principal:

1. Click one of the radio buttons *User*, *Group*, or *Role*.
2. Open the selection dialog box by clicking ...
3. Select an entry from the list displayed.
4. Click the *OK* and *Next* button.

This initial assignment makes it possible to access the new website via the Content client. All other users, groups, and roles that are to work with the new website must be assigned to it. This is done in the *User*

administration view of the Admin client (see section “Website Assignments” on page 156).

Confirm your entries by clicking the *Next* button.

Step 3 – Specify URL and Directory for Master Content Server

Different views of each website are available. These views are generated by the respective deployment systems: Edit, QA, and Production view. In the case of a minimum installation of a website, deployment systems for Edit, QA, and Production are installed on the master Content server. To keep the data for the different deployment systems separate, different directories on the computer hosting the master Content server are used to store the data.

For editing the WCM objects with the Content client and displaying the pages in a browser, the objects are accessed by means of a URL. For this purpose, an HTTP server that maps the deployment system directories to the relevant URLs must be installed on the computer hosting the master Content server. In addition, you will require a JSP engine for the Content client. Alternately, the master Content server can be executed as a web application in an application server. For information on the configuration of HTTP server, JSP engine, and application server, refer to the Livelink WCM Server Installation Manual.

The windows for entering URL and directory for the master Content server differ, depending on whether you create the website with the option *Minimum* or *Minimum (dynamic)*.

In the last dialog box of the wizard, the information is supplemented by the names of the individual deployment systems. At this point, you only need to enter the basic component of URL and directory. The resulting directory names and URLs are only suggestions and can be changed in a later step of this wizard.

Notes

- Once the website has been created, it is no longer possible to change these settings. To do this, you would have to delete the deployment systems and add them again.
- If the website objects are to be edited with the Content client, you must specify the fully qualified host name (including domain) in the base URL for the Edit and QA deployment systems. Otherwise, it is not possible to use the Content client to edit the website over the Internet. The URL for starting the Content client must also contain the fully qualified host name.
- The base URLs for Edit and QA deployment systems must not differ in uppercase and lowercase letters alone.

URL and directories for master Content server when selecting the option *Minimum*

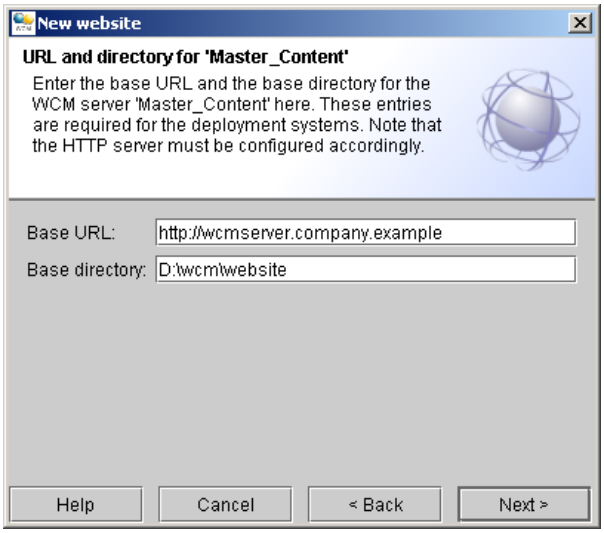

New website
URL and directory for 'Master_Content'
Enter the base URL and the base directory for the WCM server 'Master_Content' here. These entries are required for the deployment systems. Note that the HTTP server must be configured accordingly.
Base URL:
http://wcmserver.company.example
Base directory:
D:\wcm\website
Help
Cancel
< Back
Next >

Fig. 65 – Specifying base URL and directory for master Content server

In this window, you enter the *Base URL* (HTTP address) for accessing the data of the master Content server's deployment systems and the *Base directory* for storing the data.

Example

- *Base URL* = **http://wcmserver.company.example**

  This URL will be supplemented automatically by the name of the deployment system which you enter in the next dialog box. In a minimum installation, this might result in the following URLs for accessing the deployment system data:

  Edit view: **http://wcmserver.company.example/InternetSite_edit**

  QA view: **http://wcmserver.company.example/InternetSite_qa**

  Production view: **http://wcmserver.company.example/InternetSite_prod**

- *Base directory* = **d:\wcm\website**

  The data for the deployment systems is stored in the directory **\website** in the WCM installation directory. In a minimum installation, three subdirectories are created in this directory, one each for the Edit, QA, and Production deployment systems. By default, the names of these subdirectories consist of the names of the website and the deployment systems:

  Edit deployment system: **d:\wcm\website\InternetSite_edit**

  QA deployment system: **d:\wcm\website\InternetSite_qa**

  Production deployment system: **d:\wcm\website\InternetSite_prod**

> **Note:** Possible separators in the path of the base directory are forward slashes "/" and backslashes "\". You must use the separators corresponding to the operating system of your server.

URL and directories for master Content server when selecting the option *Minimum (dynamic)*

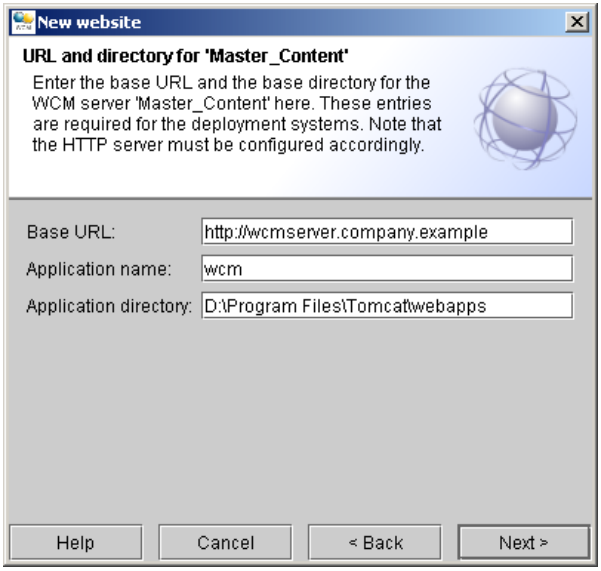

New website
URL and directory for 'Master_Content'
Enter the base URL and the base directory for the WCM server 'Master_Content' here. These entries are required for the deployment systems. Note that the HTTP server must be configured accordingly.
Base URL:
http://wcmserver.company.example
Application name:
wcm
Application directory:
D:\Program Files\Tomcat\webapps
Help
Cancel
< Back
Next >

Fig. 66 – Specifying base URL, application name, and application directory for master Content server

If you create the new website with the option *Minimum (dynamic)*, you can specify the base URL, as well as the application name and application directory of the respective web application.

- *Base URL* = **http://wcmserver.company.example**

  This URL is supplemented by the entry for the deployment system. In case of a minimum dynamic installation, the following URLs for

accessing the data of the deployment systems may result. For the Edit and QA views, the directory name **vipdyn** is inserted.

Edit view: **http://wcmserver.company.example/{application name}/vipdyn/InternetSite_edit**

QA view: **http://wcmserver.company.example/{application name}/vipdyn/InternetSite_qa**

Production view: **http://wcmserver.company.example/{application name}/InternetSite_prod**

- *Application name* (only if an application server is used): name of the web application under which the selected Content server runs in the application server. The application name is specified during creation of the web application for the application server, see “Generating a Web Application”.

  Example: wcm

  If you do not use an application server, but work with a separate JSP engine, such as ServletExec, leave this line empty.

- *Application directory:* base directory for storing the pages generated for the WCM objects. This entry is automatically supplemented by the name of the deployment system. The application directory must be located on the computer on which the selected Content server is installed. Possible separators in the path of the base directory are forward slashes “/” and backslashes “\”. You must use the separators corresponding to the operating system of your server.

  Example: d:\wcm\website

  If the Content server runs in an application server, specify the associated application directory, e.g. **C:\Program Files\Tomcat\webapps**.

Confirm your entries by clicking the *Next* button.

Step 4 – Specify Names of Deployment Systems

Now define the names of the deployment systems for the Edit, QA, and Production views. These names must be unique within the entire WCM system. You cannot change the names once the website has been created.

These names are appended to the base URLs and base directory or application directory that you specified in the previous steps. All the resulting URLs and directory names are displayed in the dialog box. These are merely suggestions; you can still change any of the entries in this dialog box.

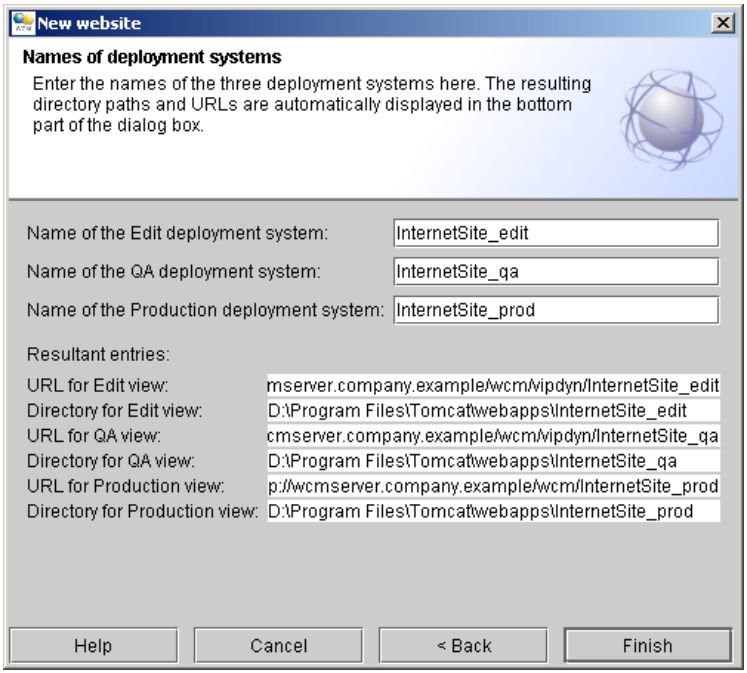


Fig. 67 – Specifying names of deployment systems

Notes

- The resulting URLs must be unique within the entire WCM system. Moreover, the computers in question must not have any directories with the same names and paths as the ones specified for the deployment data directories.
- The base URLs for the different views must not differ in uppercase and lowercase letters alone.
- In the configuration of your HTTP server, you map the names of the directories containing the generated pages to a URL. When doing this, you must use the same specifications for URL and directory as when you created the website. Otherwise, the generated pages cannot be accessed via HTTP and users cannot edit the WCM objects with the Content client.

  For information on the configuration of the HTTP server, refer to the Livelink WCM Server Installation Manual.
- After setting up the website, you can specify additional properties of the deployment systems, e.g. a URL for deleted objects. See section “Settings of Deployment Systems” starting on page 276

Confirm by clicking the *Next* or *Finish* button.

Creating a Website with the Option *User-defined*

If you chose the option *User-defined* for creating a new website, you must – as for minimum installation – first determine the website name, specify the database connection used, and assign an initial principal (see “Step 1 – Specify Website Name and JDBC Pool” on page 207 and “Step 2 – Assign a User, Group, or Role” on page 210).

You will then be asked whether you want to close the wizard or continue making specific entries for configuring the website. If you close the wizard, the website will merely be configured on the specified master Content server. No proxy Content servers will be assigned and no deployment systems will be configured. You can, however, do this subsequently in the *Configuration* view.

If you continue to create the website, the next step is to specify the proxy Content servers on which the website is to be available.

Step 3 – Assign Proxy Content Servers and Select Data Storage

In the third step, you select the proxy Content servers that you want to assign to the website.

Click the *Add* button to select the servers to be assigned to the new website from the list of available servers. This opens the *Select proxy Content server* dialog box.

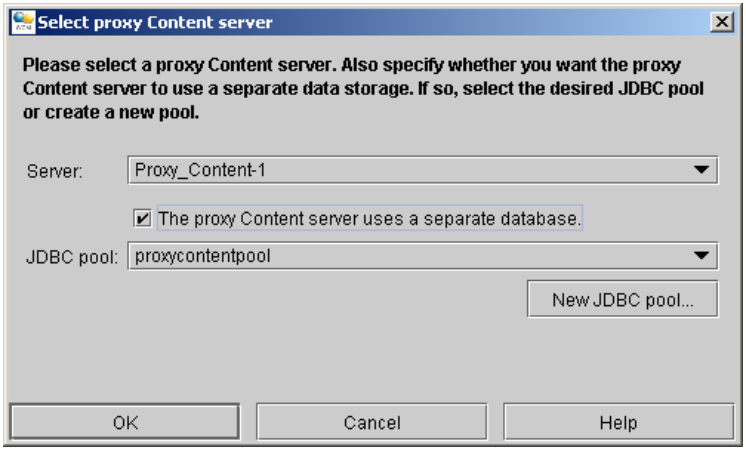

Select proxy Content server
Please select a proxy Content server. Also specify whether you want the proxy Content server to use a separate data storage. If so, select the desired JDBC pool or create a new pool.
Server:
Proxy_Content-1
The proxy Content server uses a separate database.
JDBC pool:
proxycontentpool
New JDBC pool...
OK
Cancel
Help

Fig. 68 – Configuring proxy Content servers for the website

- *Server:* Select one of the installed servers from the list.
- *The proxy Content server uses a separate database:* If the master Content server and the proxy Content server are to use the same database connection, leave the check box cleared. If the proxy Content server is to use a different database connection than the master Content server (i.e. the data is to be replicated there), select the check box. In that case, additional fields will appear:
  - *JDBC pool:* Select the desired pool for the proxy Content server from the list.
  - *New JDBC pool:* If a pool for this database connection does not exist yet, you can add a pool by clicking this button. The wizard for new JDBC pools starts.

Confirm the information about the proxy Content server by clicking the *OK* button.

Repeat this process until you have selected all the proxy Content servers for the new website.

Note: For editing the objects of the website with the Content client, at least one of the assigned Content servers must run in the context of a JSP engine or as a web application in an application server.

The overview now shows all the servers selected.

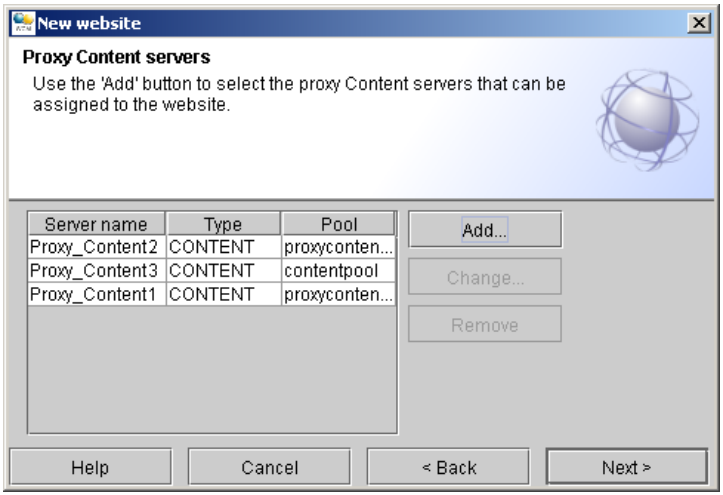


Fig. 69 – Overview of all selected proxy Content servers

Click the *Change* button to change the entries for a proxy Content server, or click the *Remove* button to delete a proxy Content server from the list.

Confirm your entries for the proxy Content servers for the new website by clicking the *Next* button.

Step 4 – Define Routing between the Servers

In the next dialog box, you specify which Content servers are to notify each other about changes to WCM objects and which data storage view is to be transmitted. For general information on routing, refer to section “Routing Between the Servers” on page 47.

In a distributed system, it may be useful to adapt the routing to the situation in the LAN or WAN because of differences in data transfer rates or firewall scenarios.

To change the routing:

1. Mark a server in the table and click on the entry in the *View* column.
2. In the *Select website view* dialog box, mark the desired view in the list.
3. Confirm by clicking the *OK* button.

> **Note:** Please note that the view determines the volume of transferred data. For example, a proxy Content server outside the company network should only have the Production view of the website data in order to reduce the volume of transferred data.

4. Click on the *Sending server* column.

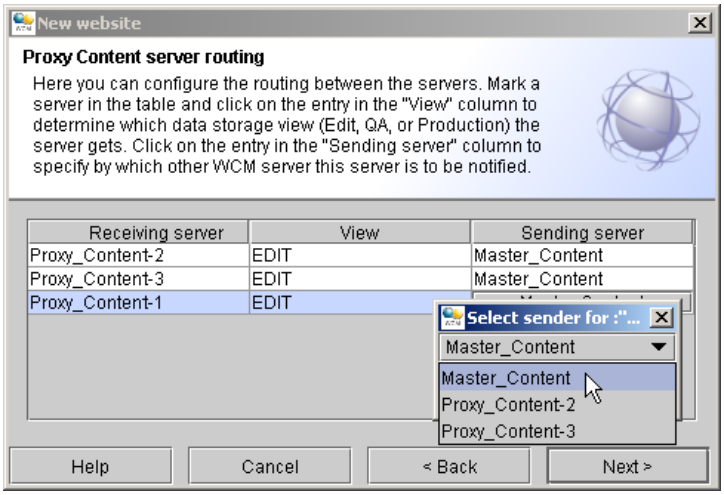

New website
Proxy Content server routing
Here you can configure the routing between the servers. Mark a server in the table and click on the entry in the "View" column to determine which data storage view (Edit, QA, or Production) the server gets. Click on the entry in the "Sending server" column to specify by which other WCM server this server is to be notified.
Receiving server
View
Sending server
Proxy_Content-2
EDIT
Master_Content
Proxy_Content-3
EDIT
Master_Content
Proxy_Content-1
EDIT
Select sender for :"...
Master_Content
Master_Content
Proxy_Content-2
Proxy_Content-3
Help
Cancel
< Back
Next >

Fig. 70 – Defining the routing

5. In the *Select sender* dialog box, mark the desired sender in the list.
6. Confirm by clicking the *OK* button.
7. Confirm your settings by clicking the *Next* button.

If you want to add the deployment systems for the new website at this stage, click the relevant radio button in the next dialog box.

If you click the *Do not add deployment systems* radio button in this dialog box, the new website is configured on the specified servers. Without deployment systems, however, it is neither possible to edit the website using the Content client nor to publish it. You can add deployment systems subsequently in the *Configuration* view.

Step 5 – Add Deployment Systems

If you specified that you want to configure deployment systems now, the *Deployment systems* dialog box opens. This dialog box shows whether deployment systems are configured for the selected Content server.

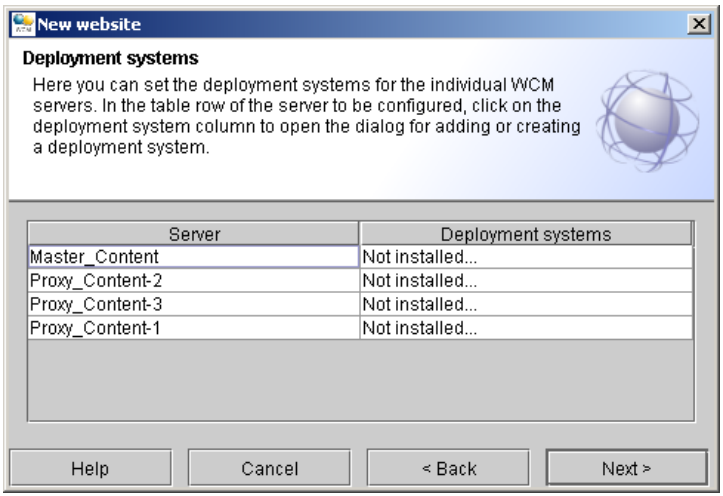

New website
Deployment systems
Here you can set the deployment systems for the individual WCM servers. In the table row of the server to be configured, click on the deployment system column to open the dialog for adding or creating a deployment system.
Server
Deployment systems
Master_Content
Not installed...
Proxy_Content-2
Not installed...
Proxy_Content-3
Not installed...
Proxy_Content-1
Not installed...
Help
Cancel
< Back
Next >

Fig. 71 – Website servers without deployment systems

To add a deployment system for a server or edit existing entries:

1. In the *Deployment systems* column of the desired server, click on the entry *Installed* or *Not installed*.

   The next dialog box (*Deployment systems of server*) shows the individual deployment systems for the selected server.

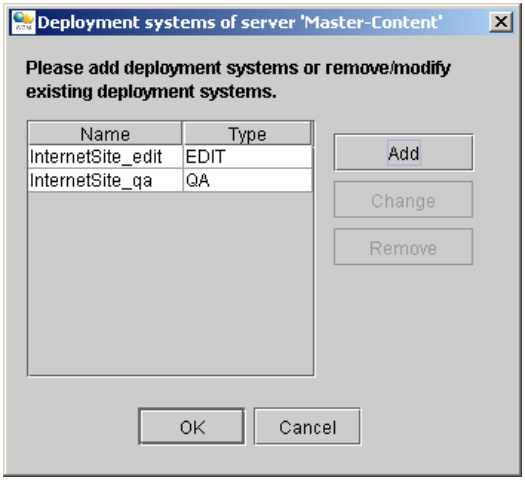


Fig. 72 – Overview of the deployment systems for a server

2. Click the *Add* button to set up a new deployment system for this Content server.

   To edit the settings of an existing deployment system, click the *Change* button.

   The wizard for adding a deployment system starts. Unlike the minimum configurations, this allows you to make extended settings, such as threads and statification, while you are creating the website.

3. Follow the instructions of the wizard.

   For a description of the individual steps in the deployment system wizard, refer to the online help on the wizard.

Notes on adding deployment systems

- **Categories** of deployment systems: Dynamic, WebDAV, and InSite Editing deployment systems can only be installed on servers running in the context of a JSP engine or as a web application in an application server. Search engine deployment systems cannot be added until the website has been created, as it is necessary to know the object types and the metadata of the website.
- **Types** of deployment systems (Edit, QA, Production): Depending on the available view of a server, you can only create certain deployment systems. For example, on a server that only has the QA view of the website data, only QA and Production deployment systems are possible. For a WebDAV deployment system, the respective server must have the Edit view.
- You may also create a new website without deployment systems. However, in this case, the new website can neither be edited with the Content client nor can it be used for productive operation. If you want users to edit the website with the Content client, you must set up an Edit and a QA deployment system (if a dynamic deployment system is used for the Content client, an Edit deployment system is sufficient).

4. Click the *Change* button to edit the settings for the deployment system in the *Deployment systems of server* dialog box, or click the *Remove* button to delete it from the list.
5. Confirm your entries for the deployment systems of an individual server by clicking the *OK* button.

   Repeat the procedure described for each server. The *Deployment systems* dialog box shows you an overview of all deployment systems configured.

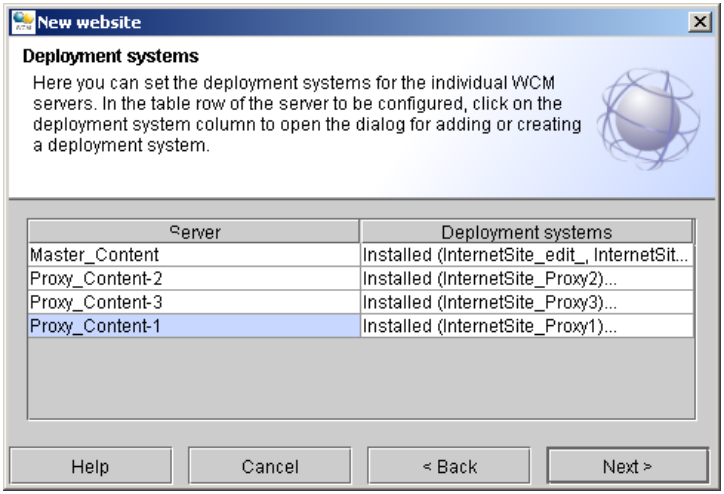

New website
Deployment systems
Here you can set the deployment systems for the individual WCM servers. In the table row of the server to be configured, click on the deployment system column to open the dialog for adding or creating a deployment system.
Server
Deployment systems
Master_Content
Installed (InternetSite_edit_, InternetSit...
Proxy_Content-2
Installed (InternetSite_Proxy2)...
Proxy_Content-3
Installed (InternetSite_Proxy3)...
Proxy_Content-1
Installed (InternetSite_Proxy1)...
Help
Cancel
< Back
Next >

Fig. 73 – Overview of existing deployment systems

6. Confirm your entries for the deployment systems by clicking the *Next* button.

Step 6 – Finish Creating the Website

The next dialog box (*Summary*) draws attention to possible sources of errors, e.g. if no deployment systems were added to the website.

You can now finish creating the new website by clicking the *Finish* button.

The proxy Content servers will be assigned and the deployment systems will be configured in accordance with your entries. The master Admin server informs the assigned Content servers about the configuration changes, and transfers the new configuration data. Directories for the deployment systems are created on the specified computers for subsequent distribution of the website data.

You can administer the new website in the *Configuration* view. Configuring websites involves:

- general settings, see section “General Website Settings” on page 226
- assignments, see table “Assignments of websites” on page 202

In the *User administration* view, you can assign users, groups, and roles to the website, thus granting them access to the website, see section “Website Assignments” on page 156

General Website Settings

To view the general settings of a website, select the website via *Configuration* → *Websites*. The settings are shown in the right window pane on the tabs *General* and *Routing*.

The settings on the *General* tab are defined when setting up the website. You cannot change them subsequently. You can only modify the caching parameters.

On the *Routing* tab, you can see the ways used by the servers to notify each other about changes. If you want to change the routing to optimize communication between the servers in order to take account of conditions in your LAN or WAN, you must remove the proxy Content server from the website assignments, then reassign it with different routing specifications. For further information, see section “Proxy Content Servers Assigned to a Website” on page 228.

Deployment Systems of a Website

Select *Configuration* → *Websites* → *{website name}* → *Deployment systems* for an overview of the deployment systems that generate the pages for the WCM objects and make these files available on the Content servers. The deployment systems are displayed in a list in the right window pane.

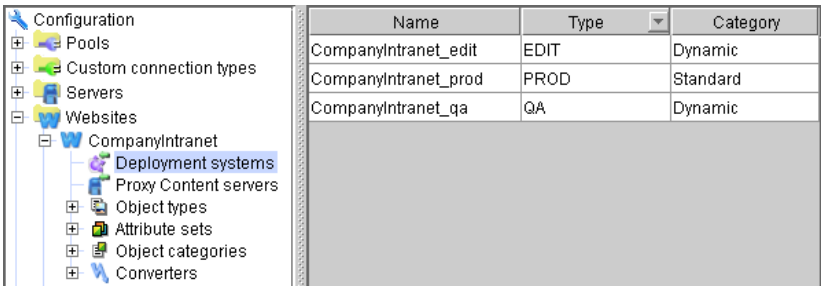


Fig. 74 – Overview of the deployment systems for a website

Deployment systems are set up during the creation of websites and managed via *Configuration* → *Deployment systems* (see chapter 8 “Managing Deployment Systems”).

Here, you can add deployment systems for the Content servers that are assigned to the selected website.

To start the wizard for adding a deployment system, choose *New deployment system* on the context menu or click this icon (see section “Adding a Deployment System” starting on page 275).

Proxy Content Servers Assigned to a Website

Select *Configuration* → *Websites* → *{website name}* → *Proxy Content servers* to display an overview of the proxy Content servers on which the selected website is available in the right window pane.

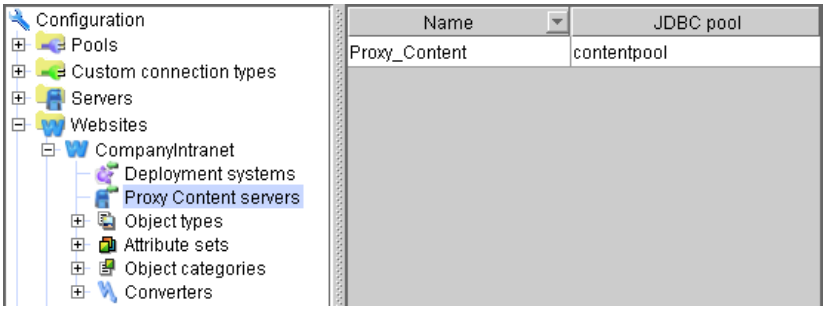


Fig. 75 – Proxy Content servers assigned to a website

Proxy Content servers are assigned to a website when the website is created. The wizard automatically adds the deployment systems on the assigned servers.

In practice, it may become necessary to assign additional proxy Content servers, e.g. to distribute the load of editing WCM objects or accessing the published website to several servers.

To assign an additional proxy Content server to a website or to remove the assignment, choose the appropriate function on the context menu or the toolbar.

Icon for assigning a proxy Content server to a website, see “Creating Assignments” on page 109

Icon for removing the assignment of a proxy Content server to a website, see “Removing Assignments” on page 112

Proxy servers can also be assigned to websites via *Configuration* → *Servers* → *{server name}* → *Websites*. The procedure is identical. Please note the information in section “Websites Assigned to Servers” on page 177.

Managing Object Types of Websites

Each WCM object is linked with a specific object type. The object type is defined when the object is added in the Content client. There are only a few cases in which it may subsequently be changed. An object’s type depends on its content and on its use. For example, regarding the content, there is no difference between a topic object and an HTML object. The topic, however, has an additional organizational function in the object hierarchy because it can accommodate other (child) objects.

By default, the default object types are linked with a default functional area. To view this assignment, select a functional area in the *User administration* view. The assignment enables you to control which users are allowed to add, check out, and check in this type of object. The precise attributes of object types are determined by the attribute set that you assign to the object type. You can also configure the attribute sets to suit your requirements, see section “Managing Attribute Sets of Websites” on page 234.

Object types are managed separately for each website. After a new website has been created, the default object types are available. To view the list of object types, select *Configuration* → *Websites* → *{website name}* → *Object types*. The object types are shown on the left in the tree structure and on the right as a list. To view the settings for an individual object type, select it in the tree on the left.

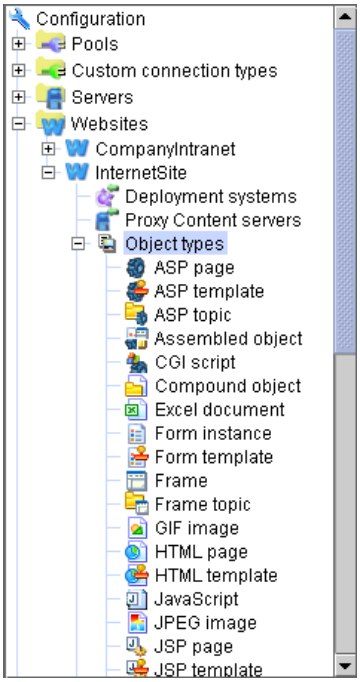


Fig. 76 – Overview of available object types

> **Note:** For a detailed description of the default object types, refer to the Content Client User Manual.

The following functions are available to you:

- adding an object type, see “Adding an Object Type” on page 231
- editing object type settings, see “Object Type Settings” on page 231
- deleting an object type from the website settings, see “Deleting an Object Type” on page 233

Adding an Object Type

In addition to the default object types, you can configure custom object types.

> **Notes:**
>
> In the Content client, the object type of WCM objects can be changed subsequently for selected object types. This is **not** possible for custom object types.
>
> In theory, you can add the object type “XML topic”. However, Livelink WCM Server does not support such an object type at present.

To add an object type:

1. Select *Configuration* → *Websites* → *{website name}* → *Object types*.
2. Choose *New object type* on the context menu or click the corresponding icon.

   Icon for adding an object type

3. Follow the instructions of the wizard. For detailed information on the individual parameters for the new object type, refer to the online help of the Admin client.

Object Type Settings

To change the settings of an object type:

1. Select *Configuration* → *Websites* → *{website name}* → *Object types*.
2. Mark the desired object type in the tree on the left.

In the right window pane, three tabs with the settings for the object type will be displayed. All these properties were defined when the object type was added. You can modify the following parameters subsequently.

- *General* tab*: Icon* and *Comment*.
- *Object data type and further settings* tab*:* all entries except the object data type
- *Assignments* tab*:* all entries, i.e. assignment of an attribute set and a functional area

For detailed information on the individual parameters, refer to the Admin client's online help.

3. Make the desired changes.
4. Click the *Apply* button.

Notes on changing object types

- If you assign a different attribute set to an object type and WCM objects with this object type already exist, the attributes and values no longer assigned are removed from the metadata of the relevant WCM objects. The removed attributes and the associated values remain stored in the database as long as no changes are made to the newly assigned attribute set for the relevant WCM objects.

  Thus, if you accidently assign the wrong attribute set and then correct your mistake immediately without any changes being made to the metadata for the relevant WCM objects, the old values will be available again.

- The servers of the WCM system are automatically notified about changes to the object types, with the result that new icons are available in the Content client, for example. However, if you installed Admin clients on computers where no WCM server exists, the changes are not available there.

Deleting an Object Type

Notes:

You can only delete an object type if no **current** versions of objects exist in the Edit, QA, or Production view that use this object type. Older versions of the objects with this object type may, however, exist.

If an object version is restored that uses the deleted object type, the object type will also be restored. A (deleted) object type is finally removed by the utility *Database clean-up* if there are no older object versions that use this type.

To delete an object type:

1. Select *Configuration* → *Websites* → *{website name}* → *Object types*.
2. Mark the desired object type in the tree on the left.
3. Choose *Delete object type* on the context menu or click the corresponding icon.

   Icon for deleting an object type

4. Confirm the security prompt by clicking the *Yes* button.

Managing Attribute Sets of Websites

Attributes describe special properties of object types. They are grouped in attribute sets that are – like object types – managed separately for each website. These attributes supplement the standard metadata of WCM objects and are displayed on the *Attributes* tab in the Metadata dialog box of the Content client.

Some of the object types generated during creation of the website are by default assigned to attribute sets. You can change this assignment for existing object types. When adding an object type, you can optionally assign an attribute set.

The attributes managed in attribute sets may, for example, be the resolution of graphics (integer), the associated editor (string), or a copyright notice (string). Each WCM object is linked with an object type, which means it possesses the attributes of the attribute set that has been assigned to the object type. By means of WCM tags, the values of these attributes can automatically be entered in the generated pages. For further information on attributes and WCM tags, refer to the Content Client User Manual.

To view the attribute sets available for a website, select *Configuration* → *Websites* → *{website name}* → *Attribute sets*. The attribute sets for the default object types are added automatically during installation: “compound”, “dynamic”, “html”, “image”, and “other”.

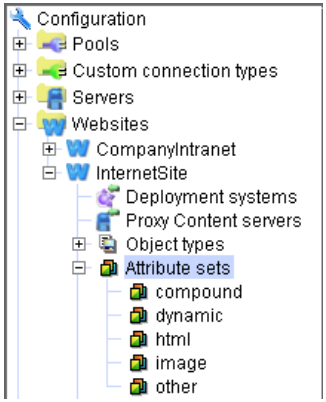


Fig. 77 – Default attribute sets

The following functions are available to you:

- adding an attribute set to a website, see “Adding an Attribute Set” on page 236
- displaying the settings of an attribute set; adding and removing individual attributes, see “Settings of Attribute Sets” on page 236
- removing an attribute set from the website settings, see “Deleting an Attribute Set” on page 237

Note: If the proxy Content servers assigned to the respective website use separate data storages, changes to attribute sets must also be saved there. For this reason, the system checks whether these proxy Content servers are available and whether the JDBC pools assigned can be used. If this is not the case, an error message is displayed and the changes to the attribute sets cannot be saved.

Adding an Attribute Set

To configure a new attribute set:

1. Select *Configuration* → *Websites* → *{website name}* → *Attribute sets*.
2. Choose *New attribute set* on the context menu or click the corresponding icon.

   Icon for adding an attribute set

3. In the next steps, you specify the name of the attribute set and assign new or existing attributes to it.

   Follow the instructions of the wizard. For detailed information on the individual parameters for the new attribute set, refer to the online help of the Admin client.

Settings of Attribute Sets

To edit the settings of an attribute set:

1. Select *Configuration* → *Websites* → *{website name}* → *Attribute sets*.
2. Mark the desired attribute set in the tree on the left.

   The settings displayed are made when the attribute set is added.
3. On the *Attributes* tab, you can use the buttons to add existing attributes to the attribute set, create new attributes, or remove attributes from the set.

   You cannot change existing attributes subsequently.
4. Click the *Apply* button.

Deleting an Attribute Set

Note: You can only delete attribute sets that are not used by any object in the relevant website.

To delete an attribute set:

1. Select *Configuration* → *Websites* → *{website name}* → *Attribute sets*.
2. Mark the desired attribute set in the tree on the left.
3. Choose *Delete attribute set* on the context menu or click the corresponding icon.

   Icon for deleting an attribute set

4. Confirm the security prompt by clicking the *Yes* button.

Managing Object Categories of Websites

By means of object categories, you categorize your WCM objects according to their content. For example, you might have categories such as “Invoice” or “Article_description”. Object categories are defined by a number of properties that you can specify yourself. Invoices, for example, could be characterized by properties such as “invoice_recipient”, “invoice_amount”, or “payment_deadline”.

When adding a WCM object with the Content client, you can optionally assign the object an object category. It then possesses the properties that you defined for this category in the Admin client. These properties supplement the standard metadata of WCM objects and are displayed on the *Properties* tab in the Metadata dialog box of the Content client.

By means of WCM tags, the values of these properties can be automatically entered in the generated pages and, for example, queried when searching a website. This would make it possible to show customers all their unpaid invoices, for example. Object categories also form the basis for assembled objects (Content Assembly). For information on properties, WCM tags, and assembled objects, refer to the Content Client User Manual.

Immediately after the installation of Livelink WCM Server, there are no object categories.

The following functions are available to you:

- adding an object category, see “Adding an Object Category” on page 238
- adding properties to existing object categories or delete properties, see “Settings of Object Categories” on page 239.
- deleting an object category, see “Deleting an Object Category” on page 240

Note: If the proxy Content servers assigned to the respective website use separate data storages, changes to object categories must also be saved there. For this reason, the system checks whether these proxy Content servers are available and whether the JDBC pools assigned can be used. If this is not the case, an error message is displayed and the changes to the object categories cannot be saved.

Adding an Object Category

To add an object category:

1. Select *Configuration* → *Websites* → *{website name}* → *Object categories*.

2. Choose *New object category* on the context menu or click the corresponding icon.

   Icon for adding an object category

3. In the next steps, you specify the name of the object category and create the properties of the object category.

   Follow the instructions of the wizard. For detailed information on the individual parameters for the new object category, refer to the online help of the Admin client.

Settings of Object Categories

To edit the settings of an object category:

1. Select *Configuration* → *Websites* → *{website name}* → *Object categories*.
2. Mark the desired object category in the tree on the left.

   The settings displayed are made when the object category is created.

3. On the *Properties* tab, you can use the buttons to subsequently create new properties and add them to the object category as well as delete properties.

   You cannot change existing properties subsequently. If you want to change a property, delete it and then create it again.

4. Click the *Apply* button.

Deleting an Object Category

> **Note:** You can only delete object categories that are not used by any object in the relevant website.

To delete an object category:

1. Select *Configuration* → *Websites* → *{website name}* → *Object categories*.
2. Mark the desired category in the tree on the left.
3. Choose *Delete object category* on the context menu or click the corresponding icon.

Icon for deleting an object category

4. Confirm the security prompt by clicking the *Yes* button.

Assigning Converters to Websites

Processing source files that are not available in HTML format is an important function of content management systems. For this purpose, Livelink WCM Server offers the possibility to integrate external conversion programs. A converter can, for example, be used to generate a set of HTML pages from word processor documents. The source files are saved together with the generated files as one complex.

Select *Configuration* → *Websites* → *{website name}* → *Converters* to integrate external conversion programs. With the help of these programs, you can convert files that are managed as WCM objects to HTML or other formats that can be displayed by a web browser. This makes it possible to

have conversions performed automatically by Livelink WCM Server. You do not have to leave the WCM environment to do this.

Prerequisites for the use of converters

For automatic conversion of files, it is necessary to install a suitable conversion program. You can basically use programs that

- can run in the operating system used for the master Content server
- can be started using a command line interface
- can be ended automatically after successful conversion

You can use any converter that satisfies these requirements. The results of the conversion and hence the quality of the generated files depend on the conversion program chosen and its configuration. The conversion program is installed and configured in accordance with the individual manufacturer's instructions.

Note: Conversion programs are not supplied with Livelink WCM Server.

Conversion process

When you add an object, you can select a source file as the content of this WCM object. In the Content client, conversion of the source file is started manually by choosing *Object* → *Convert*. This can be done at any time during the editing process.

The files generated by the converter are imported by Livelink WCM Server. When you select a source object in the Content client or Content client (Classic), a hyperlink to the source document appears in the object preview. In the tree, the files generated by the converter are shown at the same level as the source object and can be displayed in the object preview.

Available functions for converters

The following functions are available to you:

- integrating a converter, see “Configuring a New Converter”
- editing settings of a converter, see “Converter Settings”
- removing a converter from the WCM system, see “Deleting a Converter”

Configuring a New Converter

To integrate an external conversion program in the WCM system:

1. Select *Configuration* → *Websites* → *{website name}* → *Converters*.
2. Choose *New converter* on the context menu or click the corresponding icon.

   Icon for configuring a new converter

3. Follow the instructions of the wizard. The exact parameters for the converter are described in the online help of the Admin client.

Converter Settings

To change the settings of a converter:

1. Select *Configuration* → *Websites* → *{website name}* → *Converters*.
2. Mark the desired converter in the tree on the left.

   In the right window pane, three tabs with the settings for the converter are displayed. All these properties were defined when the converter was set up. Except for the file extension, you can change all parameters subsequently.

For detailed information on the individual parameters, refer to the Admin client's online help.

3. Make the desired changes.
4. Click the *Apply* button.

Deleting a Converter

To delete a converter:

1. Select *Configuration* → *Websites* → *{website name}* → *Converters*.
2. Mark the desired converter in the tree on the left.
3. Choose *Delete converter* on the context menu or click the corresponding icon.

Icon for deleting a converter

4. Confirm the security prompt by clicking the *Yes* button.

Reassigning Orphan Objects

> **Note:** To perform this function, you need the administration right “Change system status”.

When editing users, groups, and roles, you might delete principals that are already entered in the Content client as authorized to access certain WCM objects. Changes that you make in the user administration of the Admin client, of the Livelink system, or in the LDAP system are not transmitted automatically to the Content client.

This can result in the existence of WCM objects without a valid access control list (ACL), e.g. if you have deleted the only principal allowed to access an object, or if the list only contains principals who do not have read rights for the object and are not allowed to change the access rights. These objects are called “orphan objects”.

To reassign orphan WCM objects:

1. Choose *Collect orphan objects* on the *Tools* menu.

   The *Collect orphan objects* dialog box is displayed.

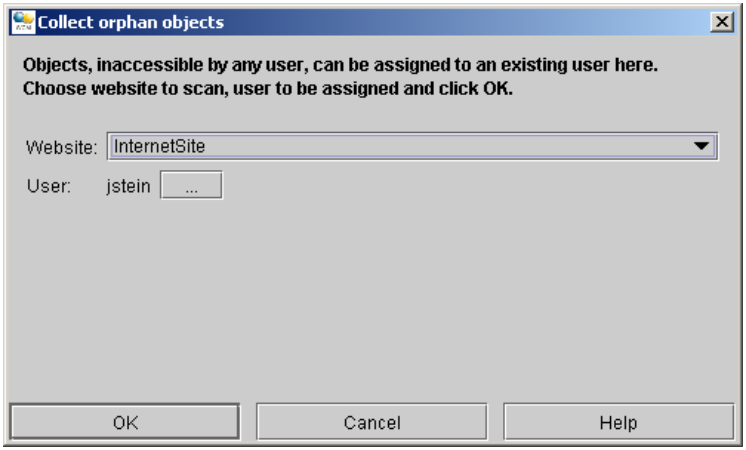


Fig. 78 – Dialog box for assigning orphan WCM objects

2. Select the desired website and the user who is to have full access to the WCM objects found.

   By means of the Content client, this user can then update the access control list for the relevant objects.

3. Confirm by clicking the *OK* button.

Once you have reassigned the user, an information window is displayed showing the OIDs of the edited WCM objects. This information is also written to the log **{server name}_out.log** of the master Content server of the website (see “Server Logs” on page 329).

Note: The modified access rights of the objects only apply to the Edit view. For the changed objects to become available in the QA and Production views, use the filter ”special access rights“ in the Content client to find these objects and then submit and release them.

Deleting a Website

Notes:

Before you delete a website, make sure that it is not being accessed by any user. In the *System administration* view, you can monitor the logged-in users and log out users.

If you want to delete your website as part of a restructuring operation on your WCM system, you can back up the website data by exporting the website first (see section “Exporting and Importing Websites” starting on page 246).

To delete a website:

1. Select *Configuration* → *Websites*.
2. Mark the desired website in the tree on the left.
3. Choose *Delete website* on the context menu or click the corresponding icon.

Icon for deleting a website

4. Confirm the security prompt by clicking the *Yes* button.

   The website is removed from all assigned servers. The WCM objects are removed from the database and the directories of the deployment systems are deleted from the computers.

Exporting and Importing Websites

Livelink WCM Server offers you the possibility to export and import websites. This enables you, for example, to preserve your website data when restructuring your WCM system or integrate parts from another website.

The following functions are available to you:

- exporting and importing complete websites via a graphical user interface or the console, see “Export and Import of Complete Websites” starting on page 247
- exporting and importing website subtrees via the console, see “Export and Import of Website Subtrees” starting on page 258

Note: When the import of websites or website parts is complete, refresh the views in all open Admin clients. In this way, the current website data is loaded into the client and you can modify the configuration.

Export and Import of Complete Websites

The export and import of websites is performed by an external program, the *Export/Import Tool*. You can use the graphical user interface or work with the console. The parameters for the export and import are configured via the user interface or in the file **export-import-conf.xml** in the directory **\admin** of the WCM installation directory.

Exported Website Data

The Export/Import Tool saves the system data of the website as XML files. These XML files are protected against manipulation by means of a checksum. The following information on the websites is stored in the XML files:

- general information on the website (name, master Content server, and JDBC pool)
- attribute sets, object types, and object categories
- WCM objects belonging to the website, including all metadata and content data
- principals directly assigned to the website (users, groups, and roles) – if these principals do not yet exist in the target system during the import, they are added automatically. The default password “vip” is used.

  The system automatically assigns the website to existing principals.

Notes

- Information on the proxy Content servers assigned, the routing information, and the configuration of the deployment systems is **not** saved. You must make these settings manually after importing the website.

- The Export/Import Tool saves the website data in the file system of the master Content server. The Export/Import Tool can be called from any computer that can establish a connection to the master Content server.
- If some objects of the exported website reference objects from a Livelink system, the system also exports the name of the pool used for managing the connections to the Livelink system. Before importing the website, make sure that a Livelink pool with this name exists in the WCM system which references the correct Livelink system. Assign this pool to the Content servers on which the imported website is to be available. Otherwise, the references to the Livelink objects become invalid.
- In case of a Livelink user administration: Livelink does not differ between groups and roles – there are only groups. If the exported website contains a group name which is already used for a role of the target system, the import will not add the new group automatically. The same applies to role names which exist as group names in the target system.

Prerequisites for Export and Import

The two server agents “WebsiteExport” and “WebsiteImport” are responsible for exporting and importing websites. Both agents are automatically set up when Livelink WCM Server is installed, and are assigned to the master Content server.

The user who carries out the export or import must log in to the WCM system and must possess the following administration rights.

Administration rights required for export

- Access to configuration
- Read access to user administration (API)

Administration rights required for import

- Create, modify, delete configuration entry
- Create, modify, delete principal
- Change assignment to website/functional area

Export and Import of Complete Websites via the Graphical User Interface

Tip: To ensure that the information on available websites, JDBC pools, and master Content server is available as soon as the graphical user interface starts, enter the connection parameters for the master Content server in the configuration file **export-import-conf.xml** in the directory **\admin** of the WCM installation directory *before* starting the Export/Import Tool. For security reasons, the password should remain empty. See table “Entries in the export-import-conf.xml file” on page 254.

Step 1 – Start the Export/Import Tool

Start the graphical user interface of the Export/Import Tool with the **exportimport.bat** file, which is located in the subdirectory **\admin** in the WCM installation directory.

Step 2 – Specify connection parameters

Before exporting or importing, check the connection parameters of the master Content server and enter the user information for accessing the server. To do so, choose *Connection parameters* on the *Operations* menu.

In the *Connection parameters* dialog box, make the entries for the desired master Content server.

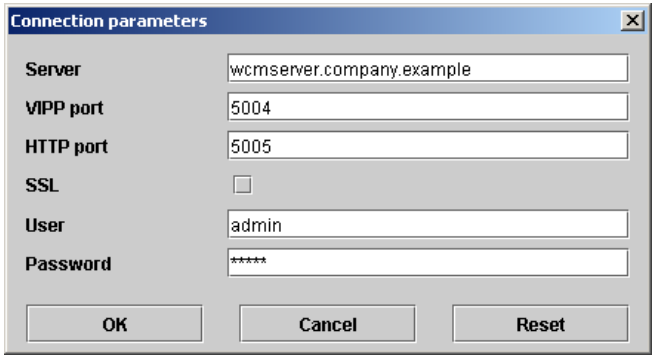


Fig. 79 – Connection parameters for the master Content server

- *Server:* name of the computer hosting the master Content server
- *VIPP port* and *HTTP port* for the connection to the master Content server
- *SSL:* If communication with the master Content server is performed via a secure connection, select this check box. This must correspond to the current settings of the master Content server.
- *User ID* and *Password* for accessing the WCM system. The user specified must have the necessary rights for export and import (see “Prerequisites for Export and Import” on page 248).

Step 3 – Specify parameters for the export

After defining the connection parameters, you can select the website that you want to export. These entries are made on the *Website export* tab of the Export/Import Tool.

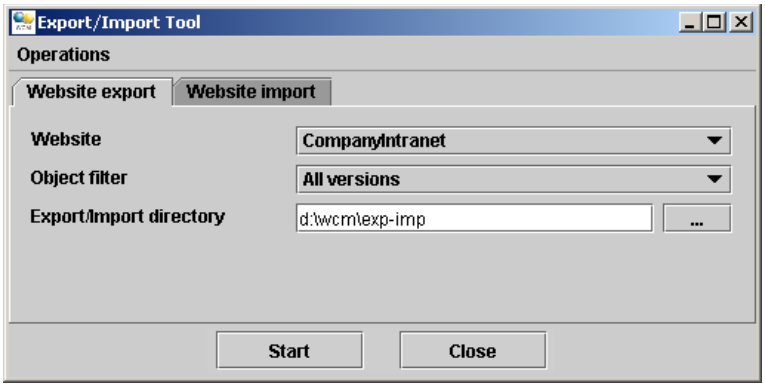


Fig. 80 – Information for exporting a website

- *Website:* From the list, select the website that you want to export.
- *Object filter:* This setting specifies which versions of which WCM objects are to be exported from the database:
  - *All versions:* all versions of all WCM objects
  - *Currently released versions:* the current version of the WCM objects in the Production view
- *Export/Import directory:* Specify the path to the directory on the master Content server in which you want to store the exported data.

  If the Export/Import Tool was started on the computer hosting the master Content server, click the button ... to select the directory. Otherwise, enter the path manually.

Start the export by clicking the *Start* button.

Note: The export results are logged in the file **{name of master Content server}_[website name}_{time stamp}.log** in the directory **{WCM installation directory}\log\exportimport**.

Step 4 – Specify parameters for the import

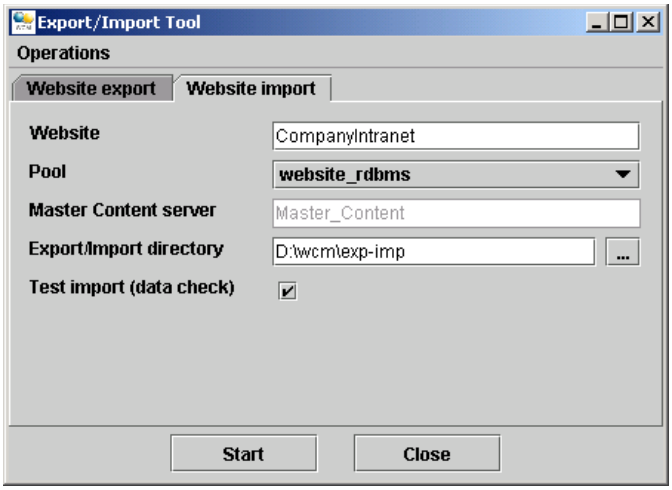


Fig. 81 – Information for importing a website

On the *Website import* tab, you can enter the following information for the import:

- *Website:* name of the website to be imported. You can keep the old name of the exported website (if it is not used yet) or enter a new name for the imported website.
- *Pool:* Select the JDBC pool for the database connection that you want to use for storing the data of the imported website.
- *Master Content server:* name of the connected master Content server (see “Step 2 – Specify connection parameters” on page 249)
- *Export/Import directory:* Enter the path to the base directory of the website to be imported.

  If the Export/Import Tool was started on the computer hosting the master Content server, click the button ... to select the directory. Otherwise, enter the path manually.

- *Test import (data check):* The test import checks whether problems are to be expected during the website import. In this mode, no data is written to the database. If errors occur, the import operation will not be cancelled (this differs from the actual import).

  Select this check box to verify the data to be read during the import.

Start the import by clicking the *Start* button.

Notes:

The (test) import results are logged in the file **{name of master Content server}_[website name}_{time stamp}.log** in the directory **{WCM installation directory}\log\exportimport**.

If errors occur when importing the website, the new website may be created anyway. In this case, use the Admin client to manually delete the website, see section “Deleting a Website” on page 245

Export and Import of Complete Websites via the Console

To automate exports and imports of websites (e.g. for backup purposes), you can also control the Export/Import Tool via the command line.

Information in the file export-import-conf.xml

Before the Export/Import Tool is called, the necessary parameters must be entered in the file **export-import-conf.xml**. This file is located in the subdirectory **\admin** within the WCM installation directory.

The XML file consists of three main sections:

1. `<vip:connection>`: parameters for the connection to the master Content server of the website
2. `<vip:export-import-operation-spec name="export-website">`: information for exporting the website
3. `<vip:export-import-operation-spec name="import-website">`: information for importing the website

The following table explains the entries in these three main sections that you must modify according to your system before the export or import.

Table 9 – Entries in the export-import-conf.xml file

Line in the XML file **Explanation**
`<vip:connection>` Section for the connection parameters to the master Content server
`<vip:server-host>localhost</vip:server-host>` The entry `localhost` must be replaced with the name of the computer hosting the master Content server. If the imported website is managed on a different master Content server, this entry must be modified accordingly before the import.
`<vip:server-vipp>5004</vip:server-vipp>` VIPP port for the connection to the master Content server using the “VIPP” protocol
`<vip:server-http>5005</vip:server-http>` Port for the HTTP connection to the master Content server
`<vip:secure>false</vip:secure>` If the connection to the master Content server uses a secure connection (SSL), `true` must be entered here.
`<vip:server-user>admin</vip:server-user>` User ID of the user who performs the export or import. This user must have the necessary administration rights, see “Prerequisites for Export and Import” on page 248.
`<vip:server-password>adminadmin</vip:server-password>` Password of the user specified above

Line in the XML file	Explanation
`<vip:export-import-operation-spec name="export-website">`	Section with the information required for the export
`<vip:req-website>website</vip:req-website>`	Name of the website to be exported
`<vip:req-filter>0</vip:req-filter>`	This entry specifies which versions of which WCM objects are to be exported. 0 = all versions of all WCM objects 1 = the current version of the WCM objects in the Production view
`<vip:req-directory>d:\wcm\exp-imp</vip:req-directory>`	Path to the directory on the master Content server in which the exported data is to be saved
`<vip:exp-protocol>false</vip:exp-protocol>`	Here you determine whether the log of the exported WCM objects is to be exported as well. If you specify `false` here, the log is empty after the import.
`<vip:reset-version>false</vip:reset-version>`	If you specified that only the current version of the WCM objects is to be exported (`<vip:req-filter>` parameter), you can use this parameter to specify the new version number for the objects. `edited` = the objects get the number 0.0.1 `released` = the objects get the number 1.0.0
`<vip:reset-author>Admin</vip:reset-author>`	Use this parameter to reset the author of the exported WCM objects to the specified value.

Line in the XML file	Explanation
`<vip:export-import-operation-spec name="import-website">`	Section with the information required for the import
`<vip:req-website>website</vip:req-website>`	Name of the website to be imported. You can keep the old name of the exported website or give the imported website a new name.
`<vip:req-directory>d:\wcm\exp-imp\website</vip:req-directory>`	Path to the base directory of the imported website
`<vip:req-pool>DB_pool</vip:req-pool>`	JDBC pool for the database connection for storing the data for the imported website
`<vip:req-master-content-server>Edit </vip:req-master-content-server>`	Name of the server that is to act as the master Content server for the imported website.
`<vip:test-import>false</vip:test-import>`	The test import checks whether problems are to be expected during the website import. In this mode, no data is written to the database. If errors occur, the import operation will not be cancelled (this differs from the actual import). `true` = perform test import `false` = no test import

Starting the export from the command line

1. Open the prompt.
2. Switch to the WCM installation directory and open the subdirectory **\admin**.
3. Enter `exportwebsite.bat`.

   This starts the Export/Import Tool. The information needed for export is read from the file **export-import-conf.xml**.

> **Note:** The export results are logged in the file **{name of master Content server}_[website name}_{time stamp}.log** in the directory **{WCM installation directory}\log\exportimport**.

Starting the import from the command line

1. Open the prompt.
2. Switch to the WCM installation directory and open the subdirectory **\admin**.
3. Enter `importwebsite.bat`.

   This starts the Export/Import Tool. The information needed for import is read from the file **export-import-conf.xml**.

> **Notes:**
>
> The import results are logged in the file **{name of master Content server}_[website name}_{time stamp}.log** in the directory **{WCM installation directory}\log\exportimport**.
>
> If errors occur when importing the website, the new website may be created anyway. In this case, use the Admin client to manually delete the website, see section “Deleting a Website” on page 245

Export and Import of Website Subtrees

Website subtrees are exported and imported by means of the external Export/Import Tool for website subtrees (`SubtreeExportImportTool`), which is called via scripts. Enter the parameters for the export and import in the file **subtree-exp-imp-conf.xml** in the subdirectory **\admin** of the WCM installation directory. For information on starting the tool, refer to section “Starting the Export of the Website Subtree” on page 268 and “Starting the Import of the Website Subtree” on page 268.

Exported Website Data

The Export/Import Tool saves the system data of the website as XML files. These XML files are protected against manipulation by means of a checksum.

> **Note:** The Export/Import Tool for website subtrees saves the website data in the file system of the computer on which the tool is started.

The export and import of website subtrees is different from the export and import of complete websites because the structure of the source and target website may be different. For example, there may be different object categories, attribute sets, or object types in the website from which you export a subtree. Moreover, the OIDs of the exported WCM objects must be changed during the import because the OIDs might already exist in the target website.

The Export/Import Tool processes the website data as follows:

- **Start OID:** The export starts from an OID that you enter in the configuration file **subtree-exp-imp-conf.xml**. This WCM object must be a released topic and may not be of the object type “Compound object”.

For import, you specify in the configuration file the OID in the target website under which the imported WCM objects are to be located. This object must also be a topic and may not be a compound object.

- **Structural information:** The attribute sets, object categories and object types used by the exported WCM objects are also exported. If this structural information is defined differently in the source and target website, the structural information is synchronized with the data of the target website during the import of the respective data. See “Merging the Structural Information of Source and Target Website” at the end of this section.
- **OIDs:** During import, the exported WCM objects get new OIDs. All existing references within the exported subtree are modified accordingly.

  > **Note:** The mapping of the OIDs is logged in detail in the import log (see “Logging Export and Import” on page 268).

  OIDs that are contained in special attributes are also changed. In the parameter `<vip:oid-mapping-for>` of the configuration file **subtree-exp-imp-conf.xml**, you can enter the names of these attributes. The OIDs contained in these attributes will be replaced by the new OIDs of the target website during the import.

  OIDs that are part of the content of WCM objects (e.g. in JSP pages) cannot be modified automatically.
- **References:** By default, objects referenced by the exported WCM objects are not exported (link depth = 0). You can, however, define exceptions and specify object types that are to be exported if references to them exist. These might, for instance, be graphics that are stored centrally. If an exported WCM object contains a reference to a WCM object of one of these object types, the referenced object is also exported and stored in the special topic “ext”, which you will find in the imported subtree after the import.

References to objects outside the exported subtree that do not belong to the defined exceptions are written to a so-called correction list (file extension **.cl**). After the import, you can modify the references on the basis of the correction list, see “Required Editing After the Import” on page 269. During the import, the respective references are converted into external references.

References that are already external in the source website are adopted without changes.

- **References to Livelink objects:** If some objects of the exported subtree reference objects in a Livelink system, the system also exports the name of the pool used for managing the connections to the Livelink system. Before importing the subtree, make sure that a Livelink pool with this name exists in the WCM system which references the correct Livelink system. Assign this pool to the Content servers on which the website is available. Otherwise, the references to the Livelink objects become invalid.
- **Templates:** The templates of the exported WCM objects are also exported, even if a template cascade is used. If the templates used are located outside the exported subtree, they are stored in the special topic “ext” during the import.

  If you want to use different templates for the imported WCM objects, you can refer to the file **export.xml** to see which template was used for which WCM object of the source website. Afterwards, you can assign new templates in the target website. See also “Required Editing After the Import” on page 269.

- **ACL:** You can adopt the access control lists (ACLs) of the exported WCM objects in the target website. During the import, the system does not check whether the assigned principals exist in the target system. Alternately, you can use the parameter `<vip:inherit-acl>` in the configuration file **subtree-exp-imp-conf.xml** to determine that the ACL of the parent topic (start topic of the import) is to be used for the imported WCM objects.
- **Log:** Optionally, the log of the WCM objects can be exported (parameter `<vip:exp-protocol>` in the configuration file). Independent of this parameter, the log of the imported WCM objects contains a note on the import.
- **Versions of the exported and imported WCM objects:** The latest released version (Production view) of the website data is exported. After the import, the WCM objects get the version number 0.0.1 and are in the state “changed”.
- **Distributed data storages:** If proxy Content servers with a separate data storage exist in your WCM system, these separate data storages are also updated during the import and synchronized with the master Content server.

Merging the Structural Information of Source and Target Website

In the case of an export and import of subtrees, the structural information of the two websites might be different – object types, attribute sets, and object categories can, for example, be defined differently. You do not have to synchronize this structural information manually before the export/import. During the import of the exported subtree, the respective data of the websites is merged automatically. In the case of conflicts, the structural definition of the target website is always kept.

In the following, the exact procedure for the individual structural elements is described.

Notes:

For merging the structural information, all proxy Content servers with separate data storage must be available during the import. If merging data is not necessary, only the proxy Content servers with Edit view that have a separate data storage must be available.

Creating and changing structural information is logged in detail in the import log (see “Logging Export and Import” on page 268).

Attribute sets

- Attribute sets that do not exist in the target website are added. The required attributes for the new attribute sets are taken from the existing attributes in the target website or are created, if necessary.
- If attributes required for an imported WCM object are missing in an existing attribute set of the target website, they are taken from the existing attributes of the target website or are created.

  Notes:

  Properties from object categories and attributes from attribute sets must not have the same names. If the target website contains a property that has the same name as an attribute to be created, the attribute is renamed. The prefix “att_” is added to the attribute, thus the entire name of the attribute can, for example, be “att_property”.

  These renamings are written to the import log, see “Logging Export and Import” on page 268.

- If an attribute set of the target website contains attributes with the same name that, however, have a different data type (such as “Integer” or “String”), the system tries to convert the attribute value into the data type of the target website during import. If this fails, the data type of the target website is adopted. The value of the attribute is deleted in this case.

Object Categories

- Object categories that do not exist in the target website are added. The required properties for the new object categories are created.
- If properties required for an imported WCM object are missing in an existing object category of the target website, they are created.

> **Notes:**
>
> If a required property already exists in the target websites, but is used for a different object category, the prefix “att_” is added to the name of the property to be created, e.g “att_property”.
>
> Properties of object categories and attributes from attribute sets must not have the same names. If an attribute that has the same name as a property to be created already exists in the target website, the property is renamed (i.e. the prefix “att_” is added)
>
> These renamings are written to the import log, see “Logging Export and Import” on page 268.

- If an object category of the target website contains properties with the same name that, however, have a different data type (such as “Integer” or “String”), the system tries to convert the property value into the data type of the target website during import. If this fails, the data type of the target website is adopted. The value of the property is deleted in this case.

Object types

- Object types that do not exist in the target website are added during the import.
- Object types that already exist in the target website but are based on a different attribute set are created with a new name. “_x” is added to the name of the original object type, e.g. “logos_x”.

Groups and roles (only for Livelink integration)

Livelink does not differ between groups and roles – there are only groups. If the exported subtree contains a group name which is already used for a role of the target system, the import will not add the new group automatically. The similar procedure applies to role names which exist as group names in the target system.

Prerequisites for Export and Import

For the export and import, the respective websites must be in the run level "(8) Website read only".

The user who carries out the export or import must log in to the WCM system and must possess the following administration rights.

- Export: "Access to configuration"
- Import: "Create, modify, delete configuration entry" and "Change system status"

If the source website has a Livelink extension, the target website must also have it.

Specifying Parameters for Import and Export

Before the Export/Import Tool is called, the necessary parameters must be specified in the file **subtree-exp-imp-conf.xml**. This file is located in the subdirectory **\admin** within the WCM installation directory.

The XML file consists of three main sections:

1. `<vip:connection>`: parameters for the connection to the master Content server of the source and target website. If the websites are located on different master Content servers, the entries must be modified accordingly before performing the export/import.
2. `<vip:export-import-operation-spec name="export-subtree">`: information for exporting the website subtree

3. `<vip:export-import-operation-spec name="import-subtree">`: information for importing the website subtree

The following table explains the entries in these three main sections that you must modify according to your system before the export or import.

Table 10 – Entries in the file subtree-export-import-conf.xml

Line in the XML file	Explanation
`<vip:connection>`	Section for the connection parameters to the master Content server
`<vip:server-host>localhost</vip:server-host>`	The entry `localhost` must be replaced with the name of the computer hosting the master Content server. If the target website is managed on a different master Content server, this entry must be modified accordingly before the import.
`<vip:server-vipp>5004</vip:server-vipp>`	VIPP port for the connection to the master Content server using the “VIPP” protocol
`<vip:server-http>5005</vip:server-http>`	Port for the HTTP connection to the master Content server
`<vip:secure>false</vip:secure>`	If the connection to the master Content server uses a secure connection (SSL), `true` must be entered here.
`<vip:server-user>admin</vip:server-user>`	User ID of the user who performs the export or import. This user must have the necessary administration rights, see “Prerequisites for Export and Import” on page 264.

Line in the XML file	Explanation
`<vip:server-password>admin</vip:server-password>`	Password of the user specified above
`<vip:installdir>d:\wcm</vip:installdir>`	Installation directory of Livelink WCM Server
`<vip:export-import-operation-spec name="export-subtree">`	Section with the information required for the export
`<vip:req-website>InternetSite</vip:req-website>`	Name of the website from which a subtree is to be exported
`<vip:req-oid>253</vip:req-oid>`	OID of the start WCM object for the export. All objects located in and below this node are exported. The respective WCM object must be a released topic and may not be a compound object.
`<vip:exp-external-links>JAVASCRIPT ETC GIF JPG PNG PIC</vip:exp-external-links>`	A list of external references separated by spaces. If exported WCM objects have a reference to an object of this type and the referenced object is located outside the exported subtree, it is also exported. References of these objects to other objects are, however, not considered. The object types most frequently used for this type of references are already preset.
`<vip:exp-protocol>false</vip:exp-protocol>`	Here you determine whether the log of the exported WCM objects is to be exported, too. If you enter `false`, the log of the objects will only contain the entry that an import has been performed.

Line in the XML file	Explanation
`<vip:req-directory>d:\wcm\exp-imp</vip:req-directory>`	Path to the directory for storing the exported data. In this directory, a subdirectory with the exported data is created. The directory can easily be renamed before the import.
`<vip:export-import-operation-spec name="import-subtree">`	Section with the information required for the import
`<vip:req-website>CompanyIntranet</vip:req-website>`	Name of the target website
`<vip:req-oid>472</vip:oid>`	OID of the WCM object under which the imported subtree is to be inserted The respective WCM object must be a topic and may not be a compound object.
`<vip:oid-mapping-for>oid_attribute oid_property</vip:oid-mapping-for>`	A space-separated list of the names of the attributes in which OIDs are stored. The OIDs in these attributes are mapped to the new OIDs of the objects in the target website.
`<vip:inherit-acl>false</vip:inherit-acl>`	Specifies whether the imported subtree is to inherit the access rights of the start topic (see parameter `<vip:req-oid>`) or to adopt the access control list (ACL) of the source website. If you enter `true`, the access rights of the start topic are adopted.
`<vip:req-directory>d:\wcm\exp-imp\InternetSite_export</vip:req-directory>`	Path to the directory with the exported website data

Starting the Export of the Website Subtree

Start the export of the website subtree by means of the script **exportsubtree.bat**, which is located in the subdirectory **\admin** of the WCM installation directory.

> **Note:** By adding the parameter `-l` in the script **exportsubtree.bat**, you control the language of the logs. You can enter `en_US` for English or `de_DE` for German.

The export starts. The required data is read from the file **subtree-exp-imp-conf.xml**.

Starting the Import of the Website Subtree

Start the import of the website subtree by means of the script **importsubtree.bat**, which is located in the subdirectory **\admin** of the WCM installation directory.

> **Note:** By adding the parameter `-l` in the script **importsubtree.bat**, you control the language of the logs. You can enter `en_US` for English or `de_DE` for German.

The import starts. The required data is read from the file **subtree-exp-imp-conf.xml**.

After the import, the website is automatically shut down and then restarted. The deployment for the imported WCM objects starts.

Logging Export and Import

During both export and import, detailed logs are created that contain information and error messages. These logs are located in the directory **\log\exportimport** of the WCM installation directory.

The import log contains detailed information on the following actions:

- creation and assignment of attributes and properties for attribute sets and object categories, e.g.

  ```
  Import: Creation of field content_topic ... OK
  ```

  ```
  Import: Assignment of field popup ... OK
  ```

- update of attribute sets and object categories, e.g.

  ```
  Import: Attribute set html updated ... OK
  ```

- assignment of new OIDs for the imported objects, e.g.

  ```
  Import: New OID for object 24: 5
  ```

- OID of the topic “ext” for imported external references, e.g.

  ```
  Import: Topic 25 for external references ... OK
  ```

Required Editing After the Import

Due to the modification of the OIDs of the imported WCM objects and the adoption of the templates and the access control lists from the source website, the target website might have to be edited after a successful import.

Please check the following:

- References to objects outside the exported subtree are written to the so-called correction list (file extension **.cl**). The correction list contains the OIDs that the WCM objects had in the source website. The import log lists the new OIDs of the objects. Note the new OID and edit or delete references that have become invalid in the target website.

- If you want to use different templates for the imported WCM objects, you can refer to the file **export.xml** to see which template was used for which WCM object of the source website. Find the new OIDs of the objects in the import log and assign them the desired templates in the target website.
- If names were changed when merging the information on object types, attribute sets, and object categories of both websites, please check whether this affects the target website. See also “Merging the Structural Information of Source and Target Website” on page 261.
- When adopting access control lists (ACL) in the target website, the system does not check whether the assigned principals exist in the target system. If necessary, you must edit the access control lists of the imported objects.

CHAPTER 8

Managing Deployment Systems

The entire configuration of your WCM system is performed via the Admin client. To open the configuration, click the

tab in the Admin client.

This chapter describes how to manage deployment systems. Deployment systems generate pages for the WCM objects which are stored in the connected database. These pages can be displayed in a browser. Thus, the deployment systems ensure that the WCM objects can be edited by means of the Content client and that the website can be published on the Internet. For general information on the categories and types of deployment systems, see section “Deployment” starting on page 36.

Processing of the deployment jobs is logged (see “Server Logs” on page 329).

Generally, deployment systems are set up when a website is created. However, they can also be added subsequently, for example, if you also want to make the QA view of the website data available along with the Edit view on a Content server. Deployment systems that are not required can be deleted.

To get an overview of the installed deployment systems, select *Configuration* → *Deployment systems*.

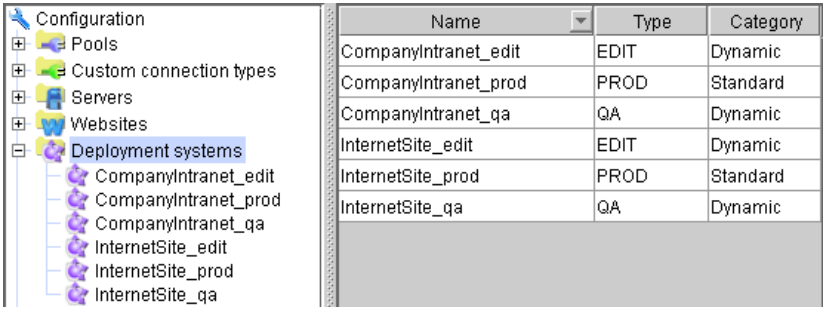


Fig. 82 – Installed deployment systems

Mark a deployment system in the tree to display the settings in the right window pane of the Admin client.

The following functions are available to you:

- setting up new deployment systems (see section “Adding a Deployment System” on page 275)
- viewing settings of deployment systems and change some settings subsequently (see section “Settings of Deployment Systems” on page 276)
- deleting deployment systems (see section “Deleting a Deployment System” on page 278)

Adding a Deployment System

To add a deployment system:

1. Select *Configuration* → *Deployment systems*.
2. Choose *New deployment system* on the context menu or click the corresponding icon.

   Icon for adding a deployment system

   The wizard for new deployment systems starts. The individual steps in the installation process depend on the deployment system **category** you install.

   - standard deployment system, see “Standard deployment system” on page 39
   - dynamic deployment system, see “Dynamic deployment system” on page 40
   - search engine deployment system, see “Search engine deployment system” on page 42
   - WebDAV deployment system, see “WebDAV deployment system” on page 42
   - InSite Editingdeployment system, see “InSite Editing deployment system” on page 43
3. Follow the instructions of the wizard. The wizard is described in more detail in the online help of the Admin client.

Settings of Deployment Systems

To view the settings of a deployment system, select it via *Configuration* → *Deployment systems* → *{name of the deployment system}*. Various tabs with the settings are displayed in the right window pane. All of these settings are made when the deployment system is set up.

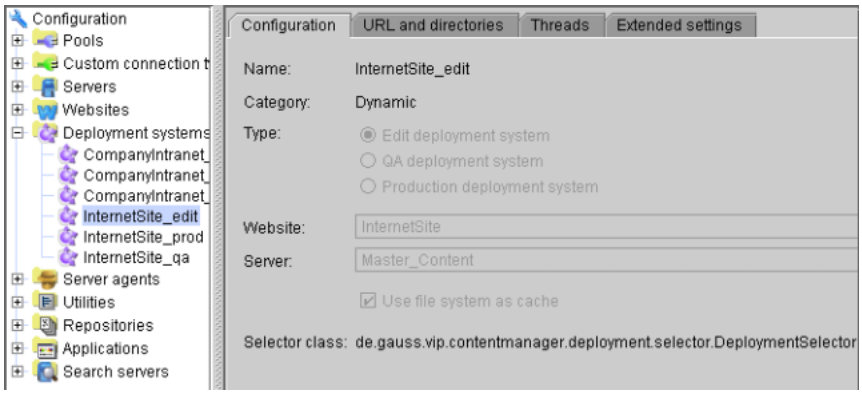


Fig. 83 – Settings of deployment systems

The type and number of the tabs displayed depends on the deployment system category. Subsequently, you can only change parameters on the following tabs. For detailed information on the individual parameters, refer to the Admin client's online help.

- *Threads:* With these parameters, you can increase the efficiency of the deployment system when generating pages.
- *URL and directories:* Select *Session settings* to change the pattern for the name and the value of the cookies used by the JSP engine for identifying the session.
- *Statification* (standard deployment system only): Here you can activate and deactivate statification. If statification is activated, the deployment system converts dynamic pages into static pages.

> **Note:** For the changes to the statification to take effect, the relevant pages must be regenerated. To start the page generation for individual objects, use the function *Regenerate page* in the Content client. The deployment agent generates pages for all objects (see “ManualDeployment” on page 294).

- *Object types* (search engine deployment systems only): The deployment systems generates only pages for the WCM objects that are based on the object types you select here.

  > **Note:** For changes to the object types to take effect, the collection must be synchronized.

- *Metadata* (search engine deployment systems only): Here you select the metadata to be indexed.

To save your changes, click the *Apply* button.

Deleting a Deployment System

To delete a deployment system:

1. Select *Configuration* → *Deployment systems*.
2. Mark the desired deployment system in the tree on the left.
3. Choose *Delete deployment system* on the context menu or click the corresponding icon.

   Icon for deleting a deployment system

   After you have deleted a deployment system, the view of website data that has been generated by this deployment system (Edit, QA or Production) is no longer available on the Content server.

CHAPTER 9

Managing Agents and Utilities

The entire configuration of your WCM system is performed via the Admin client. To open the configuration, click the

tab in the Admin client.

In this chapter the following configuration items are described:

Table 11 – Functions for the configuration of server agents and utilities

Item	Available functions
Server agents	Integrate, configure, and delete server agents, and assign agents to servers See “Managing Server Agents” starting on page 282
Utilities	Configure the utilities supplied, e.g. the database clean-up See “Managing Utilities” starting on page 310

Managing Server Agents

Server agents are Java implementations that are loaded when a server starts. Server agents run in the same runtime environment of the Java Virtual Machine (JVM) as the relevant server. The agents perform specific tasks, such as exporting or importing websites. For this purpose, they use the WCM Java API of Livelink WCM Server.

In addition to the agents that are supplied with Livelink WCM Server, you can develop agents on the basis of the WCM Java API. Via *Configuration* → *Server agents*, these agents can be integrated in the WCM system and assigned to a server. Examples of possible tasks for an agent are integrating external systems, automated processing of WCM objects, and event-controlled execution of actions. For detailed information on the functionalities provided by the WCM Java API, see the WCM Java API Programmer's Manual.

> **Note:** If agents are to access data that is managed by means of the Admin client (user information or configuration), the relevant agent must possess the necessary administration rights. See “Modifying User Assignments” on page 140 and “Modifying the Assignments of a Group or Role” on page 146.

If you open the tree item *Server agents* in the *Configuration* view, all available agents are displayed.

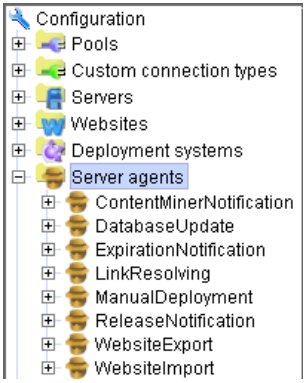


Fig. 84 – Overview of available agents

After installation you see the standard agents that are supplied with Livelink WCM Server and that are automatically integrated during the installation of a WCM system. The product also comes with additional agents that are not automatically assigned to a server. For information on all supplied agents, see section “Supplied Server Agents” on page 288.

The following functions are available for agents:

- integrate agents in the WCM system (see “Integrating an Agent” on page 284)
- configure agents by means of parameters (see “Setting the Parameters for an Agent” on page 285)
- view agent settings (see “General Agent Settings” on page 286)
- assign agents to servers (see “Assigning an Agent to a Server” on page 287)

Integrating an Agent

To integrate an agent in the WCM system:

1. Select *Configuration* → *Server agents*.
2. Choose *New agent* on the context menu or click the corresponding icon.

   Icon for integrating an agent

3. Give the new agent a unique name.

   You cannot change the name of the agent subsequently.

   > **Note:** If you want the name of the agent to be displayed in the language of the user, you can translate it (see section “Localizing GUI Texts” on page 123).

4. In the second field, enter the name of the agent’s Java class.

   The class must be accessible via the class path of the server(s) on which this agent is to run. This entry can be changed later.

5. Click the *Finish* button.

   You can now specify the parameters for the agent.

Setting the Parameters for an Agent

Agents are configured by means of parameters. The type and number of the parameters depend on the functions of the agent and its implementation.

Parameters may be defined as nodes or as individual parameters. Nodes group parameters of the same type. Nodes may contain other nodes. Unlike parameters, they do not have a value.

To define parameters for an agent:

1. Select *Configuration* → *Server agents* → *{agent name}* → *Parameters*.
2. Use the context menu or the toolbar to add a new node or parameter.

   Icon for adding a parameter to an agent

3. In the *New node* dialog box, click the appropriate radio button, depending on whether you want to add a node or an individual parameter.
4. If you clicked the *Node* radio button, enter a unique name for the new node.

   If you clicked the *Parameter* radio button, enter a name and a value for the parameter. The value may be, for example, a number or a string, depending on the implementation of the agent.

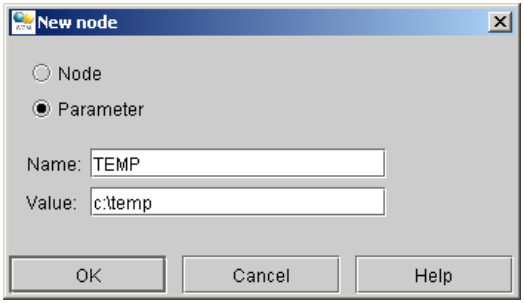


Fig. 85 – Configuring a parameter for an agent

For an example of the configuration for a node, refer to section “Specifying object types for the FileLabeling agent” on page 299.

5. Click the *OK* button.

   The parameters for the agent are now displayed under *Configuration → Server agents→ {agent name} → Parameters* and can be changed at any time.

General Agent Settings

To view the general settings of an agent, select it via *Configuration → Server agents → {agent name}*. The settings are displayed in the right window pane. You can change the name of the agent’s Java class. The agent’s name itself is defined during integration and cannot be edited later.

Assigning an Agent to a Server

Agents can only fulfill their tasks if they are assigned to a server.

Select *Configuration* → *Server agents* → *{agent name}* → *Servers*, to show the servers that the selected agent is already assigned to in the right window pane.

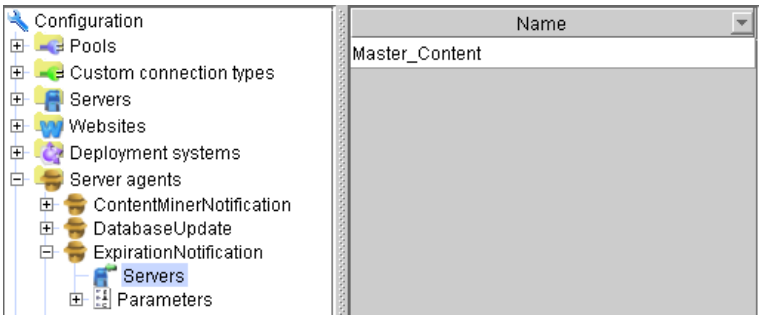


Fig. 86 – Servers assigned to an agent

The following functions are available to you on the context menu or the toolbar:

Assigning an agent to a server (see “Creating Assignments” on page 109)

Removing the assignment of an agent to a server (see also “Removing Assignments” on page 112)

An overview of the status of the agents assigned to a server is available in the system administration under *Active servers* → *{server name}* → *Agents*. You can start and stop the agents separately here. See “Assigned Agents” on page 335.

Deleting an Agent

> **Note:** You can only delete server agents that are not assigned to any server.

To delete an agent:

1. Select *Configuration* → *Server agents*.
2. Mark the desired agent in the tree on the left.
3. Choose *Delete agent* on the context menu or click the corresponding icon.

   Icon for deleting an agent

4. Confirm the security prompt by clicking the *Yes* button.

   The agent's configuration is deleted from the WCM system, but the associated Java class is not deleted.

Supplied Server Agents

Some agents are supplied with Livelink WCM Server, i.e. the relevant Java classes are installed when setting up the WCM system. Some of the agents supplied are automatically integrated in the WCM system and assigned to the respective server. Others are supplied with the product, but are not automatically integrated. The following table gives an overview of the agents supplied.

Table 12 – Overview of the server agents supplied

Server agent	Function	Automatically integrated
Expiration Notification	Automatically sends e-mails about expired objects in a website See “ExpirationNotification and ReleaseNotification” on page 290	✓
DatabaseUpdate	Repairs proxy data storages See “DatabaseUpdate” on page 292	✓
ManualDeployment	Starts the deployment on request See “ManualDeployment” on page 294	✓
ReleaseNotification	Automatically sends e-mails about objects released with a delayed release date See “ExpirationNotification and ReleaseNotification” on page 290	✓
LinkResolving	Subsequently resolves relative links See “LinkResolving” on page 295	✓
ContentMiner Notification	Synchronizes the calls between the search engine and Livelink WCM Server See “ContentMinerNotification” on page 296	✓
WebsiteExport	Exports websites See “WebsiteExport and WebsiteImport” on page 296	✓
WebsiteImport	Imports websites See “WebsiteExport and WebsiteImport” on page 296	✓

Server agent	Function	Automatically integrated
Automatic Conversion	Automatically converts WCM objects See “Automatic Conversion” on page 296	
FileLabeling	Automatically labels generated pages as executable files See “FileLabeling” on page 298	
LivelinkFolder Synchronization	Automatically synchronizes WCM topics and Livelink folders See “LivelinkFolderSynchronization” on page 302	
DefaultContent	Combines templates with standard content See “DefaultContent” on page 307	

ExpirationNotification and ReleaseNotification

These agents run on the master Content server and work for all configured websites. They are automatically assigned when a website is created.

The “ExpirationNotification” agent sends an e-mail about the expired objects in a website at a selected time. It uses the e-mail address that is entered in the metadata item *E-mail Edit* of the relevant WCM objects in the Content client.

The “ReleaseNotification” agent sends, at a specified time, an e-mail listing the objects for which a delayed release has taken place since the last e-mail was sent. It uses the e-mail address that is entered in the metadata item *E-mail Release* of the relevant WCM objects in the Content client.

Note: In the file **{WCM installation directory}\config\mail-conf.xml**, you can modify the layout of the e-mails generated by means of this agent. For detailed information on the configuration parameters of this file, refer to the online documentation (Javadoc) of the class `EMailInfo`. For the changes made in the file **mail-conf.xml** to take effect, all servers must be restarted.

Configuration

Both agents have the following parameters:

- *starttime:* time of first execution of the agent in the format 00:00 (time from 00:00 to 23:59). If the specified time has already elapsed when the server starts, the agent becomes active for the first time at the specified time on the following day. The default value is `00:00`. The time zone of the master Content server is used.
- *unit:* time unit for the parameter *interval*. Possible values are `minute`, `day`, and `hour`. The default value is `day`.
- *interval:* interval between the repeated execution of the agent. If you enter `1` here and have specified *day* under `unit`, the agent is executed once a day. The default value is `1`.

If you do not want the two agents to send e-mails, remove the assignments of the agents to the master Content server. You can also delete the agent configuration, but note that the assignment of these agents is made every time a website is created. After the creation of a new website, you must remove the assignment of the agents if you do not want automatic e-mails to be sent. If you have deleted the agents, an error message is output when the master Content server of the new website starts. However, this does not prevent the server from starting.

DatabaseUpdate

You can use the “DatabaseUpdate” agent to update the separate data storage of proxy Content servers. This may be necessary, for example, if you realize that WCM objects are missing in a proxy data storage. You can use the DatabaseUpdate agent to copy the missing data from the master data storage to the proxy data storage.

> **Note:** This agent only adds missing data. If there is already a record with the same primary key and faulty data in the database of the proxy Content server, this cannot be repaired by the agent.

The agent is integrated by default, but is not assigned to a server. If you want to use it, you must first assign it to the master Content server of the desired website, see “Assigning an Agent to a Server” on page 287. It is not necessary to configure parameters.

Working with the “DatabaseUpdate” agent

The agent is started automatically when the assigned Content server starts. You can also start the agent manually via *System administration* → *Active servers* → *{server name}* → *Agents*, see “Assigned Agents” on page 335. When the agent is started, the graphical user interface opens.

To update the separate data storage of proxy Content servers:

1. Log in to the server. For this purpose, click the following icon:

2. Enter the user ID and password for accessing the server.
3. Click a website in the drop-down list.
4. In the list next to *Proxy Content servers*, click the proxy Content server whose database you want to update. The list shows all proxy

Content servers that are assigned to the selected website and have a separate data storage.

> **Note:** If several proxy Content servers use the same database, only the proxy Content server that the master Content server notifies first about changes can be selected for a database update. The routing for the selected website is shown in the field *Routing*.

After login, the topics and pages of the selected website are displayed in a tree view in the agent window.

5. Mark the desired topic or an individual page in the tree. If you have selected a topic and also want to copy **all** child objects in this topic to the proxy database, select the *Include child objects* check box.
6. Start replication of the selected WCM objects by clicking the following icon:

The relevant WCM objects are copied from the master data storage to the proxy data storage.

7. If your WCM system uses several separate databases for proxy Content servers, repeat the process for other proxy Content servers, if necessary.
8. If the database update is complete, you can close the graphical user interface. Click the following icon:

ManualDeployment

The agent for manual deployment is used to trigger the deployment for the WCM objects of a website, i.e. to generate pages for the WCM objects.

This agent is automatically integrated, but not assigned to a server. If you want to make manual deployment available on a server, assign the agent to a server, see “Assigning an Agent to a Server” on page 287. It is not necessary to configure parameters.

Working with the agent for manual deployment

The agent is started automatically when the assigned server starts. You can also start the agent manually via *System administration* → *Active servers* → *{server name}* → *Agents*, see “Assigned Agents” on page 335. When the agent starts, the graphical user interface opens on the computer hosting the assigned server.

1. Log in to the server. For this purpose, click the following icon:

2. Enter the user ID and password for accessing the server.
3. Click a website in the drop-down list.

   After login, the topics and pages of the selected website are displayed in a tree view in the agent window.
4. In the *Available deployment systems* drop-down list, click one of the deployment systems available on this server.
5. From the tree, select the topic for which you want to generate the pages. If the marked topic includes subtopics or subordinate objects, these pages will also be regenerated.

6. Start the deployment for the selected topic and all child topics and pages by clicking the following icon:

7. If the deployment is complete, you can close the graphical user interface. For this purpose, click the following icon:

LinkResolving

The agent for resolving references is used to resolve relative references in generated pages. This functionality is needed, for example, when adding objects using a WebDAV client.

If a generated page contains a reference to another page for which no file can be found in the local file system, this reference is automatically interpreted by WCM system as an external reference. If a page is subsequently placed at the position in the file system to which the relative reference points, the agent for resolving links transforms this external reference into an internal one. In this way this reference, like all other internal references, is maintained as part of the automatic reference check by Livelink WCM Server and remains valid even when objects are, for example, moved.

The agent runs on the master Content server and works for all configured websites. It is automatically assigned when a website is created. It is not necessary to configure parameters.

If you remove the assignment of the agent to the master Content server, the external references continue to exist and are not converted into internal references. Such references cannot be included in the reference check of Livelink WCM Server.

ContentMinerNotification

This agent is automatically integrated in the WCM system when a Search server is installed or assigned to a WCM server. It is used to synchronize calls between the Search server and Livelink WCM Server.

The agent automatically determines the necessary configuration from the settings of the Search server; it is not necessary to configure parameters or assign it to a server.

WebsiteExport and WebsiteImport

These two agents are responsible for exporting and importing websites. They are automatically assigned to the master Content server when a website is created.

The export or import process is controlled by an external Export/Import Tool that is started separately. For detailed information, see section “Exporting and Importing Websites” starting on page 246.

Automatic Conversion

This agent controls the automatic conversion of objects and thus fulfills the same task as the *Convert* function in the Content client. The implementation of this function via a server agent is in particular designed for converting objects managed by means of external clients, such as a WebDAV client.

The agent for automatic conversion is supplied with Livelink WCM Server. However, it is neither set up automatically nor assigned to a server. If you want to use this agent, you must manually integrate it in the WCM system.

Integrating and configuring the agent for automatic conversion

1. Select *Configuration* → *Server agents* to integrate the agent in the WCM system (see “Integrating an Agent” on page 284). Define a name for the agent, e.g. “AutomaticConversion”.

Enter the following class name:

```
de.gauss.vip.contentmanager.server.agents.
ConvertContentAgent
```

2. In the dialog box that follows, select the website for which the agent is to act.
3. In the same dialog box, click the *Add* button to enter the parameters of the agent.

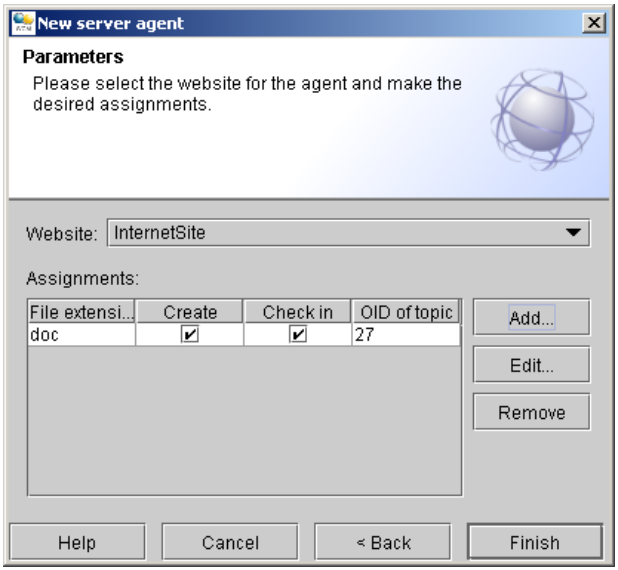


Fig. 87 – Configuring the agent for automatic conversion

First, specify the file extension of the objects to be converted and determine whether the objects are to be converted when they are added and/or checked in. Additionally, you can specify the OID of a topic. This converts only objects located below this topic.

4. Finish integrating the agent by clicking the *Finish* button.

5. Assign the new agent to the master Content server of the selected website (see “Assigning an Agent to a Server” on page 287).
6. For the agent to become active, you must start it explicitly via *System administration* → *Active servers* → *{name of the master Content server}* → *Agents*.

Notes:

In the settings for the agent on the *Parameters* tab, you can enter additional file extensions at any time.

For the changes to take effect, the agent must be restarted. This is done in the *System administration* view, see “Assigned Agents” on page 335.

FileLabeling

In some operating systems (e.g. UNIX), it is necessary to label certain files as executable in order to work with them. In the context of Livelink WCM Server, this applies to CGI scripts, among others.

To avoid the need for file labeling after the creation of such files by a deployment system, you can use the FileLabeling agent. It automates the labeling of executable files.

This agent is not automatically integrated in the WCM system. Once you have integrated the agent and assigned it to a server, the agent starts automatically when the server starts. Whenever a deployment process takes place, the agent automatically sees to the labeling of changed files. The agent processes the files of all deployment systems that are installed on a server. If there are several websites available on a server, it handles the data of all websites.

Integrating the FileLabeling agent

Select *Configuration* → *Server agents* to integrate the agent in the WCM system, see “Integrating an Agent” on page 284. Define a name for the agent, e.g. “FileLabeling”.

Enter the following class name:

```
de.gauss.vip.contentmanager.server.agents.
SetExecutableAgent
```

Specifying object types for the FileLabeling agent

1. After integrating the agent, select it and mark the *Parameters* item.
2. Use the context menu or the toolbar to add a new parameter.

Icon for adding a parameter to an agent

3. In the *New node* dialog box, click the *Node* radio button and enter “objecttypes” as the name.

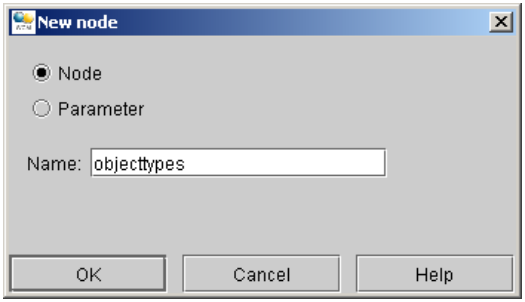


Fig. 88 – Adding a node to the FileLabeling agent

4. Click the *OK* button.

   The node is added below *Parameters*. It automatically acquires a parameter “objecttypes1”.

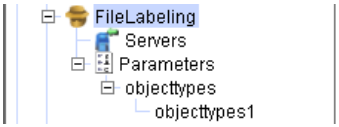


Fig. 89 – The node “objecttypes”

5. Mark the parameter “objecttypes1”.

   The settings for the parameter are displayed in the right window pane.

6. Under *Value*, enter the **internal name** of the object type for which the agent is to act, e.g. “CGI”.

7. Click the *Apply* button.

If you want to use the agent for several object types, add uniquely numbered additional parameters, e.g. “objecttypes2” and “objecttypes3”, to the node *objecttypes*. Enter the internal name of the object type as *Value*.

Specifying log options for the FileLabeling agent

The agent can log all actions that it performs on files. You can make settings for this function in the configuration. If these settings are not present, the agent’s actions are executed, but not logged.

To activate the log function, you must add the parameters listed in the table below to the agent’s configuration.

> **Important!** These parameters must not be added below the node “objecttypes”, but must be entered directly under *Parameters*.

Table 13 – Log parameters for the FileLabeling agent

Parameter	Value
`logfile`	Name of the log file, including extension Example: **labeling.log**

Parameter	Value
`logpath`	Full path to log file Example: **/home/wcmuser/WCM/log/labeling/**
`logsize`	Maximum size of log file in bytes. If this figure is exceeded, the existing log is overwritten, starting at the beginning. Example: 5000

The full configuration of the FileLabeling agent might then look like this:

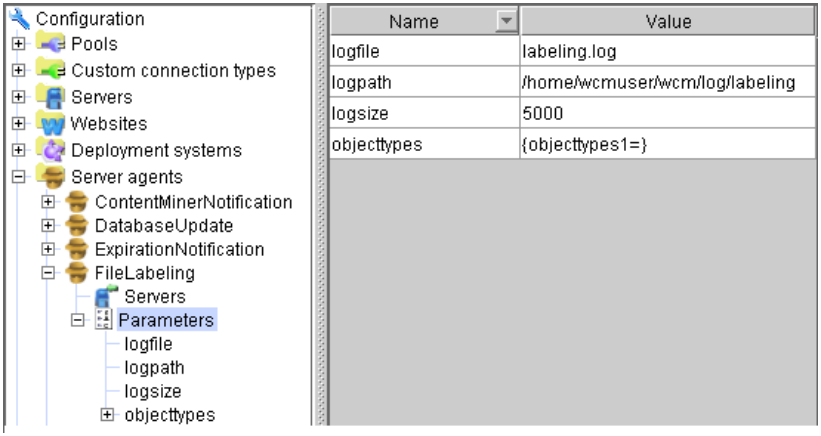


Fig. 90 – Configuring the FileLabeling agent

Assigning the FileLabeling agent to a server

After having defined the parameters for the agent, you can now assign the agent to the server on which it is to act. The agent is called automatically for every deployment process.

For information on assignments, see section “Assigning an Agent to a Server” on page 287.

LivelinkFolderSynchronization

This agent automatically synchronizes a topic of a WCM-managed website with a Livelink folder (including subfolders). It ensures that all changes in the Livelink folder are automatically transferred to the website.

If users add, delete, or modify items in the watched Livelink folder, the agent performs the corresponding actions in the assigned website topic and releases the changed or new objects. Thus, the WCM objects in the topic are no longer subject to the workflow or staging of Livelink WCM Server. You cannot manually change the WCM objects when the agent is running. The agent adds objects of type “Livelink relator”.

This agent is supplied with Livelink WCM Server as a file named **LivelinkFolderMirrorAgent.jar**. This file is located in the **\livelink** directory on the WCM CD. If you want to use the LivelinkFolderSynchronization agent, copy this file to the directory **{WCM installation directory}\external_lib** on the server on which you want the agent to run. After that, you must manually integrate the agent in the WCM system (see the following sections) and assign it to the desired server.

Integrating the LivelinkFolderSynchronization agent

Select *Configuration* → *Server agents* to integrate the agent in the WCM system, see “Integrating an Agent” on page 284. Define a name for the agent, e.g. “LivelinkSynchronization”. Enter the following class name:

```
de.gauss.agent.livelink.LivelinkFolderMirrorAgent
```

Configuring the agent

You can use the agent for multiple websites and Livelink folders. To configure the agent:

1. After integrating the agent, select it and mark the *Parameters* item.
2. Use the context menu or the toolbar to add a new parameter.

Icon for adding a parameter to an agent

3. In the *New node* dialog box, click the *Node* radio button and enter the website name as the node name.

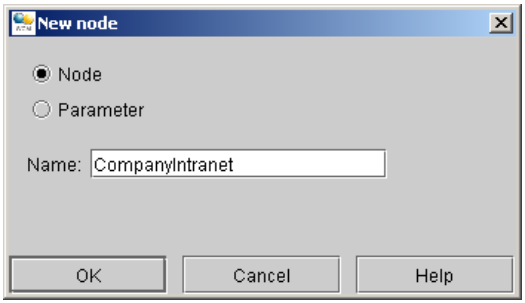


Fig. 91 – New node for LivelinkFolderSynchronization agent

4. Below the website node, add the following parameters:
   - `userId` and `userPwd`: As values, enter the login name and password for accessing the Livelink system.

     The user with this name and password must have full access rights for the corresponding topic in the WCM system (only the right “Change rights” is not required). In the Livelink system, this user must have the “See Contents” permission for the folder.
   - `systemName`: Enter the name of the connected Livelink system or the name of the corresponding Livelink pool as the value of this parameter.

> **Note:** You can also define this parameter above the website node. In this case, it applies to all websites and watched Livelink folders. You can also add this parameter below the folder node (see below) – in this case, it only applies to this individual watched folder.

The configuration below the website node could look as follows:

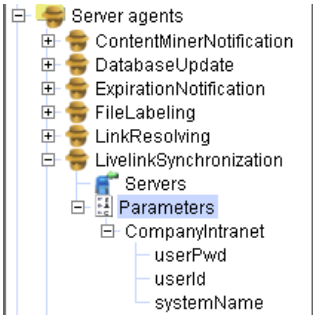


Fig. 92 – Configuration below the website node

5. Below the node with the website name, add another node for the Livelink folder which the agent is to monitor.
6. Below the folder node, add the following parameters:
   - `folder`: As value, enter the node ID of the Livelink folder which the agent is to monitor. Alternately, you can enter the path to the folder, e.g. “Enterprise:Documents”. A colon is used to separate the folder names.

> **Note:** If you enter a path, only folders of the Enterprise Workspace can be specified. If you want the agent to monitor a folder from the Personal Workspace, enter the node ID.

Any subfolders contained in the specified folder will also be monitored. The agent automatically adds topics for these subfolders.

- `topic`: As value, enter the path to the website topic which is to contain the contents of the Livelink folder. If the topic does not exist in the website, it will be added. If you enter `/Documents`, for example, the topic “Documents” will be added below the root object.

  Note: Make sure that the parent topic is released. Otherwise, the agent cannot release any objects.

- `timing` (optional): Use this parameter to specify how often the agent is to check the Livelink folder for changes. Enter a time followed by an interval.

  Examples:

  `10:00:00 every day`: The agent checks the Livelink folder once a day at 10 o'clock.

  `00:00:00 every 2 hours`: The agent checks the Livelink folder every two hours. The check starts on the hour.

  `00:30:00 every 2 hours`: The agent checks the Livelink folder every two hours. The check starts on the half hour.

  `00:00:00 every 5 minutes`: The agents repeats checking every 5 minutes (default setting).

- `topicTemplate` (optional): If the website topic for the Livelink contents is not assigned a template or is added by the agent, the agent will create an HTML template for the topic. If you want to use another template for the topic, enter the template's path or OID as the value of this parameter. In this way, you can, for instance, assign a JSP template to the topic which automatically creates a navigation for the Livelink objects.

If you specified an existing topic to which a template is assigned in the `topic` parameter, this template will be used.

The template will also be applied to all subordinate topics added by the agent.

The configuration below the folder node could look as follows:

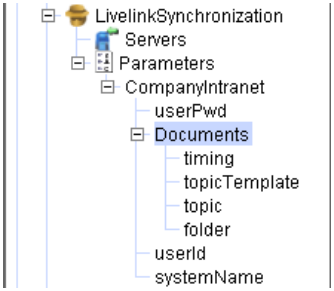


Fig. 93 – Configuration below the folder node

7. If the agent is to monitor additional Livelink folders and publish the contents on the same website, add subnodes for these Livelink folders below the website node (steps 5 and 6).
8. If you want the agent to synchronize topics in multiple websites with Livelink folders, add nodes for these websites (steps 1 to 6).
9. Assign the agent to the master Content server of the website. Start the agent via the system administration.

The agent writes its error messages to the log of the assigned Content server. If errors occur, monitoring will be cancelled automatically. To start monitoring again, restart the agent via *System administration* → *Active servers* → *{name of master Content server}* → *Agents*.

Users cannot edit the objects in the website topic manually as long as the agent is running. If you want to enable manual editing – e.g. because an error occurred – you must stop the agent.

DefaultContent

This agent is supplied with Livelink WCM Server, but is not automatically assigned to a server. If you want to use the agent for default content, you must manually integrate it in the WCM system (see “Integrating and configuring the agent for default content” on page 308).

This agent makes it possible to link templates of a website with default content, thus presetting the content of new objects to which this template is assigned. Existing WCM objects are used as default content. When a WCM object is added, the content of an existing WCM object is integrated automatically in the new object.

The agent must be assigned to the master Content server of the website. The assignment of templates and default content is done separately for each website. Thus, if you manage several websites and want to use more than one agent for default content, you must set up a separate agent for each website.

You define the parameters for the agent in the configuration. Each template of the website can be assigned a default content.

If a new WCM object without content is added in the Content client, the agent checks whether the template assigned to this object is linked with default content. If this is the case, the default content is inserted in the new object.

The function of the agent depends on several conditions. These are automatically checked by the agent when a user adds a WCM object:

- The object type of the new object must match the object type of the WCM object with the default content: for template object types, only template object types can be used. This rule also applies vice versa: For non-template object types (e.g. HTML pages), template object types may not be used as default content.

- Was a file selected as the content for the new object? In this case, the content from the selected file will be inserted instead of the default content.
- Is the template selected for the new object linked with default content in the agent's configuration?

The agent only inserts the default content in the new object if all the conditions are satisfied. If – due to these conditions – the new object cannot be linked with a default content, an entry is written to the error log of the master Content server, and the object is created without content.

Integrating and configuring the agent for default content

1. Select *Configuration* → *Server agents* to integrate the agent in the WCM system, see "Integrating an Agent" on page 284. Define a name for the agent, e.g. "InternetSite_DefaultContent". Enter the following class name:

   ```
   de.gauss.vip.contentmanager.server.agents.
   DefaultContentAgent
   ```

2. In the dialog box that follows, select the website for which the agent is to act.
3. In the same dialog box, you assign templates of a website to WCM objects, which serve as default content.

   The OIDs of the WCM objects are used to identify the templates and default content. In the following example, the WCM object with OID 5 serves as default content for objects to which the template with OID 12 is assigned, and the WCM object with OID 6 serves as default content for objects to which the template with OID 14 is assigned.

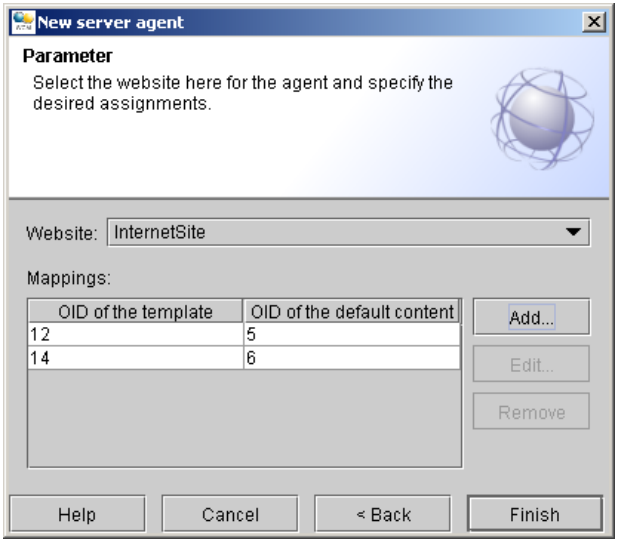


Fig. 94 – Configuring the agent for default content

4. Finish integrating the agent by clicking the *Finish* button.
5. Assign the new agent to the master Content server of the selected website (see “Assigning an Agent to a Server” on page 287).

Notes:

In the settings for the agent on the *Parameters* tab, you can enter additional OIDs of templates and default content at any time.

For the changes to take effect, the agent must be restarted. This is done in the *System administration* view, see “Assigned Agents” on page 335.

Managing Utilities

Similar to the server agents, the utilities of Livelink WCM Server perform specific tasks, such as deleting old website versions from the associated relational database. Utilities are run as threads. Threads are processes that can, in multitasking environments, be performed independently of and at the same time as other processes.

The utilities are automatically set up during the installation of Livelink WCM Server and are run by the WCM system at certain (configurable) intervals. Unlike server agents, you cannot add new programs. The utilities are run on all servers.

For an overview of the available utilities, select *Configuration* → *Utilities*.

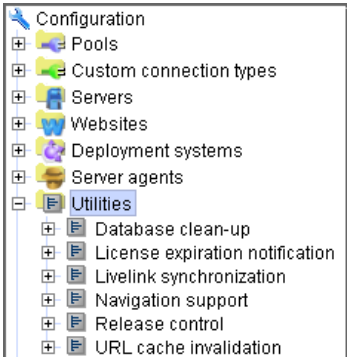


Fig. 95 – Overview of available utilities

The following table provides a brief overview of the functions offered by the utilities.

Table 14 – Utilities and their functions

Utility	Function
Database clean-up	Removes deleted WCM objects and old versions of WCM objects from the database The utility processes the master data storage and (if existing) all proxy data storages of the WCM system. For this reason, the master Content server and all servers that have a separate data storage must be active when the utility is executed. In the configuration of the utility, you can specify how many versions are to be archived in the database and at which intervals the clean-up is to be performed. For detailed information, refer to the online help of the Admin client.
Release control	Controls the release of objects with the object status “delayed release” You cannot make any further settings for this utility.
Livelink synchronization	Synchronizes relator objects when the referenced Livelink objects are modified
License expiration notification	Automatic e-mail notification if the number of active users is too high or if limited-term licenses expire In the configuration of this utility, you can set the e-mail recipient and the time settings for sending e-mails. For detailed information, refer to the online help of the Admin client.
Navigation support	Updates the internal topic structure saved in the database. This topic structure is used to speed up the search for objects in a certain topic. In the configuration of this utility, you can specify how often the internal topic structure is to be updated.

Utility	Function
URL cache invalidation	Deletes invalid object URLs from the cache of the server If WCM objects are modified, e.g. their title is changed or they are moved, the URL of the object might change. In such a case, this utility informs the Content servers that are assigned to the respective website and deletes the invalid URLs from the cache of the servers. This is done one minute after each change. You cannot make any further settings for this utility.

Notes:

You can view the status of the individual utilities via *System administration → Active servers → {server name} → Reports → ThreadManager*.

In the file **{WCM installation directory}\config\mail-conf.xml**, you can modify the layout of the e-mails generated by the Release control utility. For detailed information on the configuration parameters of this file, refer to the online documentation (Javadoc) of the class `EMailInfo`. For the changes made in the file **mail-conf.xml** to take effect, all servers must be restarted.

CHAPTER 10

System Administration

The *System administration* view provides an overview of the currently active servers and websites in your WCM system as well as of the logged-in users and their actions. You can set the servers and websites to defined run levels and cancel long-running actions.

The detailed reports and trace logs facilitate locating and resolving errors. The System administration view also offers a permanent overview of the licenses currently in use.

To open the system administration, click the

tab in the Admin client.

Fig. 96 – System administration items

The items you can manage in this view are displayed in a tree structure. The following table gives an overview of the functions available for each item.

Table 15 – Items and functions of the system administration

Item	Available functions
Active servers	Overview of the active servers in the WCM system with their associated websites, report functions, server and trace logs, actions in progress, and assigned agents Change run levels of servers and websites, cancel actions in progress, start and stop agents Generate web applications for integration with application servers See section “Administering Active Servers” starting on page 317
Registered users	Overview of users currently logged in to the WCM system and logout of individual users See section “Managing Logged-in Users” starting on page 339
Active websites	Overview of active websites and associated servers Change website run levels on all servers See section “Managing Active Websites” starting on page 341
Licenses	Overview of the licenses in use for authors, servers, websites, deployment systems, and other products of Livelink WCM Server See section “Managing Licenses” starting on page 344
Search servers	Only if Search servers are installed Start and stop Search servers, manipulate collections See Content Miner and Search Server Connector for Lucene Manuals

If you open one of the items, the Admin client will determine the current values for your WCM system, as for example the active servers. The results are shown in the right window pane.

Administering Active Servers

Select *System administration* → *Active servers* to display an overview of the servers currently active. In the right window pane, the currently running servers will be displayed with their names and run levels. If an error occurs while retrieving the run level, the message “Server not available” and the corresponding error message will be displayed.

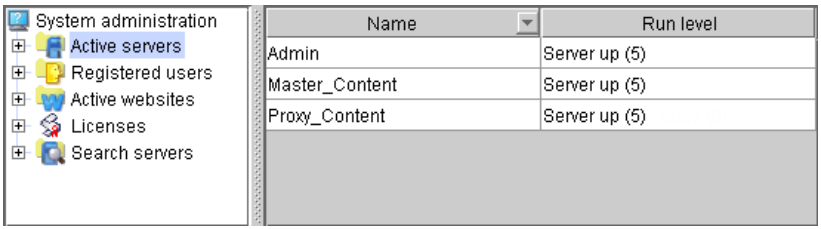


Fig. 97 – Overview of active servers

If you select one of the active servers in the tree, the settings for this server (name, type, port connections, etc.) and the server's current run level are displayed. You can set the run level here or restart the server and the assigned website(s), see “Server Run Levels” on page 318.

If you expand one of the servers in the tree, you see the other items of the server administration. The following functions are available:

- listing *Associated websites* with the option of setting the run level for the website(s) (see “Overview of the Websites of a Server” on page 323)
- viewing *Reports*, saving them, or sending them by e-mail (see “Server Reports” on page 325)
- viewing *Server logs* with messages and errors, saving them, or sending them by e-mail (see “Server Logs” on page 329)
- creating *Trace logs* (see “Trace Logs” on page 332)

- overview of *actions in progress* on the servers, canceling time-consuming actions, (see “Actions in Progress” on page 334)
- overview of agents assigned to the server, starting and stopping agents (see “Assigned Agents” on page 335)

The Admin client also offers you the possibility to generate a web application for integrating a server in an application server (see “Generating a Web Application” on page 336).

Server Run Levels

The processes running on the servers and websites are classified in so-called *run levels*. The run level is a criterion for ranking the execution of certain processes. For example, for editing WCM objects via the Content client, the highest server run level (5 “Server up”) and the highest website run level (10 “Website up”) are required. Depending on the backup software used, a particular run level might also be required for a database backup.

Run levels exist for servers and for websites. The website run levels are based on the server run levels and are only available if the respective servers are in run level 4 “Single user mode” or 5 “Server up”. If the run level of a server is further reduced, the websites are also shut down automatically.

The interdependence between website and server run levels is shown in the following table. For information on the individual website run levels, refer to section “Website Run Levels” on page 341.

The following table provides an overview of the server run levels.

Table 16 – Server run levels

No.	Name	Description	Possible website run levels
0	Server not available	The server is not available.	6 “Website inaccessible”
1	Connections closed	All communication connections are closed. Database, Livelink, and LDAP connections as well as services are no longer available. When changing to the next higher run level, connection management is established.	
2	No users logged in	No users are logged into the server. When changing to the next higher run level, user administration is activated.	
3	No agents running	All server agents are shut down. Use of the WCM Java API is not possible until the next higher run level is reached. When changing to the next higher run level, all server agents start.	6 “Website inaccessible”

No.	Name	Description	Possible website run levels
4	Single user mode	All users except the administrator who changes the run level are logged out and can no longer log in to the WCM system. This run level is especially designed for maintenance work on the WCM system. When changing to run level 3, the websites will be shut down completely. When changing to the next higher run level, the system becomes available for all users.	6 “Website inaccessible” 7 “Configuring website” 8 “Website read only” 9 “Deployment complete” 10 “Website up”
5	Server up	Startup of the server is complete.	

It may be necessary to change the run level in order to perform certain actions, such as a backup. It is also necessary to reduce and subsequently increase the run level for certain changes in the configuration to become effective. To perform maintenance work on the WCM system, you can use run level 4 “Single user mode”, which gives only one administrator access to the system.

When the run level of a server or website is reduced, new actions are not accepted if they require a higher run level. If a user attempts to perform such an action, e.g. releasing an object, the system will respond with an error message. Actions in progress are brought to completion. Thus, all the actions for a run level gradually come to an end.

When all the processes for a run level have been completed, the same procedure begins for the next run level. When a server is shut down, this procedure is repeated until all the processes on the server have been completed.

Notes:

If a shutdown of the servers is delayed by time-consuming user actions, these actions can be canceled by selecting *System administration* → *Active servers* → *{server name}* → *Actions in progress*.

When changing the run level of a Content server running in the context of a JSP engine or as a web application in an application server, no users should be accessing the website(s) of this server via the Content client. You can get an overview of active users via *System administration* → *Registered users*. You can also log out users here.

For changing the run level of servers, various functions are available in the toolbar and the context menu.

Set run level for all servers: Sets the run levels of all servers. If the servers are run down to a run level below 4 “Single user mode”, the assigned websites are shut down automatically. To make it possible to control the run levels of servers and websites separately, the websites are not started automatically when the server run level is increased again via the Admin client.

This function is available if you select *System administration* → *Active servers* in the tree on the left.

Set server run level: This function sets the run level for a selected server. Here too, the websites are not automatically started when the server is set to a higher run level.

Note: When you set down the run level of an Admin server, you can decide whether the run level of the associated servers should also be set down. If you select *No*, the run levels of the associated servers remain unchanged. While the Admin server is shut down, it is not possible to log in to the WCM system. Proxy systems (i.e. WCM systems managed by a proxy Admin server) are in general not affected by run level changes in the master system.

Restart server: By means of this function, the server is run down to a selected run level and then run up again to the original run level. The run level of the assigned websites is also restored. You can, for example, use this function to make changes to the server configuration take effect.

Note: If you restart the Admin server this way, all dependent servers will also boot until they reach the run level of the Admin server.

Notes

- You cannot run down a server to run level 1 in the Admin client, as the server cannot be restarted via the Admin client.
- If you run down a server to run level 0, it cannot be restarted via the Admin client either. In this case, use the server's start script or the appropriate function of the application server (if the WCM server runs in an application server). Starting the servers in this way also starts up the websites.
- To run down the servers step by step to run level 0 “Server not available”, you can also use the batch or shell scripts in the installation

directory. If the WCM server runs as a web application in an application server, it can be shut down with the appropriate application server function.

For more information on starting and stopping the servers, refer to the Livelink WCM Server Installation Manual.

Overview of the Websites of a Server

Select *System administration* → *Active servers* → *{server name}* → *Associated websites* to obtain information about which websites are available on a Content server and which run levels the websites have.

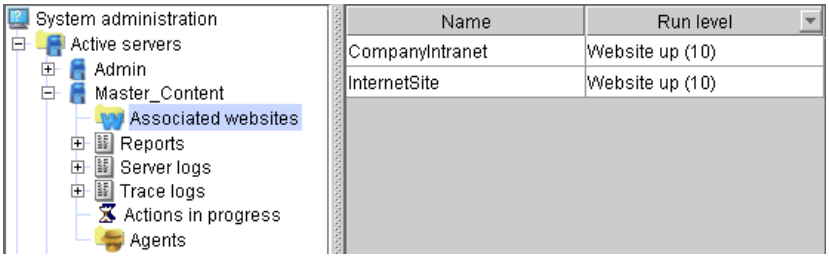


Fig. 98 – Overview of the websites of a server

Run levels exist for servers and for websites. The website run levels are based on the server run levels and are only available if the respective Content servers are in run level 4 “Single user mode” or 5 “Server up”. If the run level of a Content server is further reduced, the websites are also shut down automatically.

Here you can control the run level of a website separately for the selected server. The website’s run level on other Content servers remains unaffected. To change the website run level on all assigned servers, select *System administration* → *Active websites* (see “Website Run Levels” on page 341).

Changing the run level on a specific server might, for example, be necessary to stop the deployment on this server.

To change the run level of a website on a server:

1. Select *System administration*→ *Active servers* → *{server name}* → *Associated websites*.
2. Mark the desired website in the right window pane.
3. Choose *Set website run level* on the context menu or click the corresponding icon.

   Icon for setting the run level of websites

   The *Select new run level* dialog box opens.

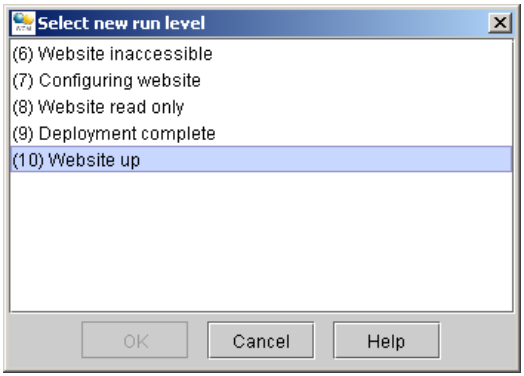


Fig. 99 – Changing the run level of a website

4. Mark the desired run level.
5. Click the *OK* button.

   For information on the individual run levels, refer to table “Website run levels” on page 342.

Note: If you change the run level of a website, users should no longer access the website via the Content client. You can get an overview of active users via *System administration* → *Registered users*. You can also log out users here.

Server Reports

Select *System administration* → *Active servers* → *{server name}* → *Reports* to open the reporting functions of Livelink WCM Server. Comprehensive reports are available for each server. They provide you with up-to-date information about actions in the WCM system. These reports can be used to analyze and resolve problems.

Depending on the type and configuration of the server, different reports are created. For example, deployment reports are only available for servers on which deployment systems have been set up.

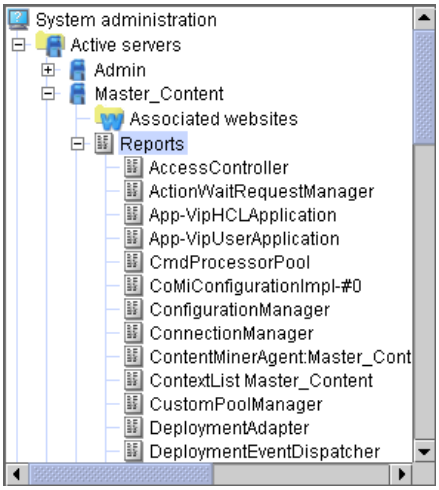


Fig. 100 – Reports available for a master Content server

The reports are created at the moment you select one of the reports in the tree.

Functions for reports

The following functions are available on the context menu and the toolbar. You can apply these functions to a selected report or all reports of a server.

Send report(s) by e-mail: sends the selected report or all reports by e-mail. The *Send e-mail* dialog box opens. In this dialog box, you can enter the recipient(s) of the e-mail. The e-mail address of the logged-in administrator is automatically used as the sender.

Save report(s): saves the selected report or all reports in text format in any directory on any drive

Update element data: updates the selected report or all reports. This may be necessary to determine the current status during time-consuming actions.

Overview of reports

The following list gives you an overview of the most important reports. For detailed information on the individual report sections, refer to the Admin client's online help.

- *AccessController Report:* This report is created for all servers for which Secure Access has been activated. See sections “General Server Settings” on page 176 and “Managing Paths for Secure Access” starting on page 186. It contains the configured Secure Access paths and an ACL tree of the website.
- *ConfigurationManager report:* The ConfigurationManager report contains a list of the internal components that are notified automatically in the case of configuration changes. If a proxy Admin server

cannot be reached in the case of a configuration change, a corresponding entry is written to the report.

- *ConnectionManager report:* This report provides information on the outbound connections of this server to other WCM components.
- *ContextList report:* All information on logged-in users is combined in the ContextList. Each server has its own ContextList. The Administration server collects all lists at regular intervals. It is thus able to provide a summary of all users in its ContextList report.
- *DeploymentAdapter report:* This report contains a list of the deployment systems installed on the selected Content server and a list of the deployment systems which are installed on other Content servers, but are accessible from this server.
- *DeploymentForwardThread report:* The report shows the status of the deployment components and statistical information on forwarding or processing deployment events and jobs.
- *DeploymentSystemHandler report:* A DeploymentSystemHandler report is created for each deployment system. It contains detailed information on orders and jobs of the deployment systems that are installed on this server.
- *DisplacingObjectCache report:*This report provides information on the performance and effectiveness of the object cache. You can specify the parameters for the object cache in the settings of the website, see “General Website Settings” on page 226 and “Step 1 – Specify Website Name and JDBC Pool” on page 207.
- *LicenseManager report:* For Content and Search servers, the LicenseManager report contains only the IP address of the respective computer as well as the name of the Administration server to which license requests are forwarded. For Administration servers, the report contains the full range of license information for Livelink WCM Server.

- *LivelinkObjectHandler report:* This report is created for each configured Livelink entry point and contains statistical information on loading Livelink objects.
- *LivelinkSystemManager report:* This report contains information on synchronizing the WCM cache for Livelink objects with the Livelink system.
- *ObjectManagerImpl report:* The ObjectManager manages all objects of a website and controls locking of objects while objects are being edited or released. It is present once for each website. The ObjectManagerImpl report contains information about WCM objects that are currently being edited and which are therefore locked for access by other users.
- *PoolManager report:* This report provides information about the pools of the WCM system.
- *ReceiverManager report:* This report logs the communication via the connections in the server's pools.
- *RunlevelManager report:* The run levels of the selected server and the websites that are available on this server are listed in this report. Moreover, the report lists the other servers of the WCM system that the selected server communicates with via WCM connections.
- *ServerAgentManager report:* This report is an overview of the agents that are assigned to the selected server.
- *ServerInfo report:* This report contains information on the installed server and the computer hosting the server.
- *ThreadManager report:* The ThreadManager controls the utilities of Livelink WCM Server. The ThreadManger report indicates whether the ThreadManager is active on the selected server. It contains information on the individual utilities.

- *VersionSupervisor report:* This report provides information on the classes or JAR files currently loaded in the server. This makes it possible to check whether all Service Packs for Livelink WCM Server are taking effect and whether the order of the JAR files in the class path is correct.

Server Logs

Select *System administration* → *Active servers* → *{server name}* → *Server logs* to view the logs of the selected servers. These logs are sorted by name, file size, and date of the last change and contain the servers' information and error messages. They are stored in the subdirectories **\log**, **\log\deployment**, and **\log\contentminer** of the WCM installation directory on the computer hosting the respective server. Like reports, the logs can be used to analyze and solve problems.

Notes:

Empty logs are not displayed in the Admin client. They are, however, saved in the respective directories.

If the parameter `-noredirect` is set in the start script of the respective server, messages are not recorded in the log files, but output to the console. For more information on the parameters of the start scripts, refer to the Livelink WCM Server Installation Manual.

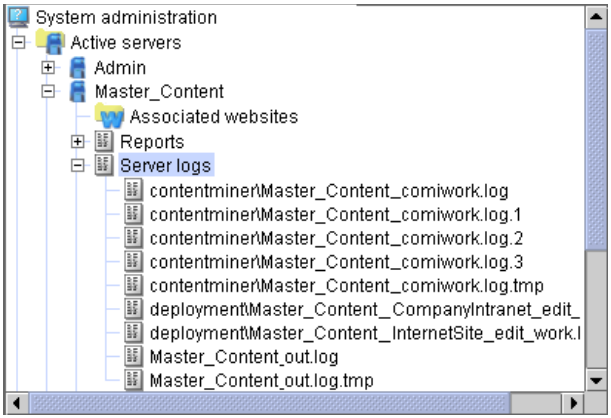


Fig. 101 – Logs available for a master Content server

The following logs are written for the different WCM servers:

- **\contentminer\{server name}_comiwork.log:** messages regarding the actions of Search servers, e.g. creating a collection. This log is only created for servers that are assigned a Search server.
- **\contentminer\{server name}_comierr.log:** error messages of Search servers
- **\deployment\{server name}_{name of the deployment system}_work.log:** messages regarding the jobs of the respective deployment system, e.g. page generation
- **\deployment\{server name}_{name of the deployment system}_err.log:** error messages of the respective deployment system
- **{server name}_com.log**: messages on communication errors. This file is only created in the case of an error.
- **{server name}_err.log**: error messages

- **{server name}_lic.log** (only for Admin servers): information on licenses used and released for servers, deployment systems, etc.
- **{server name}_out.log**: standard messages, such as changing the run level of servers or websites and starting agents

Every time a server is started, a new log file is created. If this file already exists, the complete file name of the old version is supplemented with **.1**, **.2**, etc. If the log file becomes larger than 10 MB, the file is copied (file extension **.tmp**) and a new log file is created. If this one also becomes larger than 10 MB, the first log file is deleted. Afterwards, a new file is created whenever the limit of 10 MB is exceeded. This maximum value for the size of the log files (default = 10 MB) can be set by means of the parameter `-logsize` in the start script of the server.

For the logs, the following functions are available on the context menu or the toolbar. You can apply these functions to individual or all logs of a server.

Send log(s) by e-mail: sends the selected log or all logs by e-mail. The *Send e-mail* dialog box opens. In this dialog box, you can enter the recipient(s) of the e-mail. The e-mail address of the logged-in administrator is automatically used as the sender.

Save log(s): saves the selected log or all logs in text format in any directory on any drive

Delete log(s): deletes the selected log or all logs. The current logs of the servers cannot be deleted.

Note: Creating previously deleted logs anew may be time-consuming.

Update element data: refreshes the view

Trace Logs

In addition to reports, trace logs represent an important means of finding and solving the cause of problems. Using trace logs, you can log current actions on a server, including methods calls and error and information messages.

Creating and evaluating these logs is a very time-consuming task. For this reason, it is possible to turn trace logs on and off at runtime and to set filters for tracing.

> **Note:** Trace logs should only be created and evaluated in cooperation with Gauss Interprise AG.

Switching tracing on and off

To switch on tracing for a server, select *System administration* → *Active servers* → *{server name}* → *Trace logs*. Two tabs with configuration options for tracing are displayed in the right window pane:

- On the *Global filter* tab, you can define a global filter for tracing.
- On the *Class-specific filters* tab, you can select individual Java classes of Livelink WCM Server for tracing.

  For detailed information on the individual parameters, refer to the Admin client's online help.

Make the filter settings for tracing. Tracing is activated automatically and the trace log is displayed in the tree on the left.

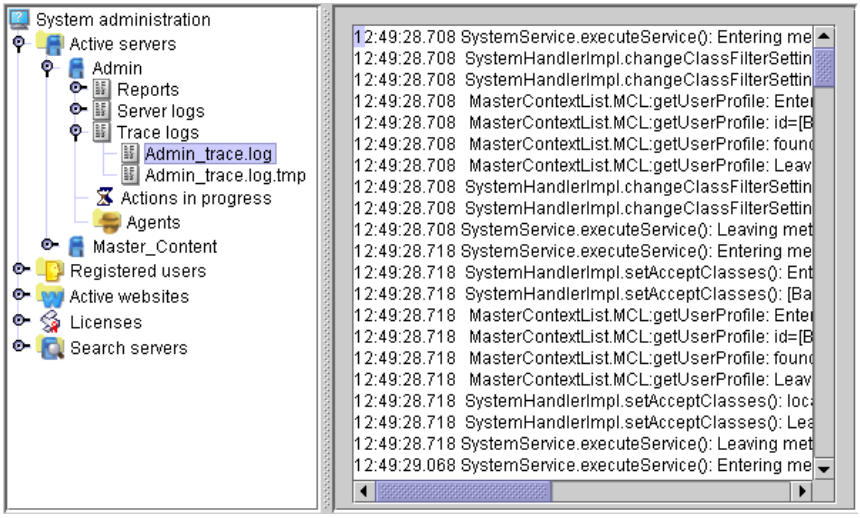


Fig. 102 – Trace log of a server

The log is saved with the file name **{server name}_trace.log** in the subdirectory **\trace** of the WCM installation directory. If the log file becomes larger than 10 MB, the file is copied (file extension **.tmp**) and a new log file is created. If this one also becomes larger than 10 MB, the first log file is deleted. Afterwards, a new file is created whenever the limit of 10 MB is exceeded.

To switch off tracing again, clear the check box for the global or class-specific filter and click the *Apply* button.

> **Note:** Internally, the tracing is activated when methods are entered or exited. For this reason, switching the tracing on and off may take effect with some delay.

Functions for trace logs

If trace logs exist, the following functions are available to you via the context menu and the toolbar:

Send log by e-mail: sends the selected log by e-mail. The *Send e-mail* dialog box opens. In this dialog box, you can enter the recipient(s) of the e-mail. The e-mail address of the logged-in administrator is automatically used as the sender.

Save log: saves the selected log in text format in any directory on any drive

Delete log: deletes the selected log. This is only possible if tracing is switched off.

Update element data: refreshes the display of the selected log. This may be necessary to determine the current status during time-consuming actions.

Actions in Progress

Select *System administration* → *Active servers* → *{server name}* → *Actions in progress* to get an overview of the actions that are currently being performed on a server. This may be the release or creation of WCM objects, for example.

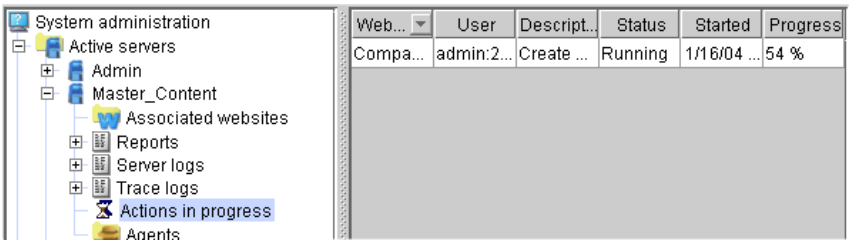


Fig. 103 – Overview of the actions in progress on a server

The following information is displayed for each action:

- website on which the action is performed
- user ID and session ID of the user performing the action
- description of the action, e.g. “Create objects”
- status, start time, and progress of the action

You can cancel time-consuming actions (or processes that are already complete, but not marked as complete) that unnecessarily delay servers from shutting down. Choose *Cancel action* on the context menu or click the corresponding icon.

Icon for canceling an action in progress

Actions that you cancel with this command are completely undone by Livelink WCM Server (rollback).

Assigned Agents

Select *System administration* → *Active servers* → *{server name}* → *Agents* to display an overview of the status of the agents that are assigned to this server. Agents are assigned to servers in the *Configuration* view, see “Assigning an Agent to a Server” on page 287.

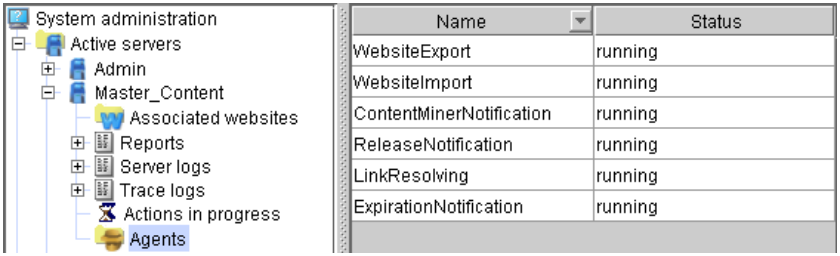


Fig. 104 – Status of the agents on a master Content server

All agents that are assigned to a server are started automatically when the server starts. This is done on transitioning from run level 3 “No agents running” to run level 4 “Single user mode”.

You can start and stop the agents **separately** here. For this purpose, select an agent in the list on the right and call the desired function via the toolbar or the context menu.

Stop agent: stops agent on this server

Start agent: starts agent on this server. This can also be done below the server run level 3 “No agents running” (down to and including run level 1). In this way, you can restart individual agents after all agents have been stopped automatically when reaching run level 3.

Notes:

When a server progresses from run level 3 to run level 4, **all** agents assigned to this server are started automatically.

Information on manufacturer and version of the assigned agents is contained in the ServerAgentManager report under *System administration → Active servers → {server name} → Reports*.

Generating a Web Application

Livelink WCM Server can be integrated in application servers. For this purpose, the servers must be executed as web applications in the application server. You can create these applications when installing Livelink WCM Server or subsequently with the Admin client. A web application contains all components required for executing the server. These include, for example, servlets, JSP pages, class libraries, JavaBeans, etc.

A so-called WAR file (web archive) is used for integrating the web application in the application server. This file is a compressed directory structure in ZIP format containing all components of a web application. This directory structure is described in the Java™ Servlet Specification, v2.2 (see http://java.sun.com). For all servers, WAR files can be conveniently created via the Admin client.

Notes:

The servers for which WAR files are to be created must be completely started. To start a Content server that usually runs in the context of a JSP engine or as a web application in an application server separately from the application server or the JSP engine, you can use the script **startserver.bat** or **startserver.sh** from the WCM installation directory. For more information on starting and stopping the servers, refer to the Livelink WCM Server Installation Manual.

For detailed information on the application servers supported, refer to the Release Notes of Livelink WCM Server.

To create a web application:

1. Select *System administration*→ *Active servers*.
2. Mark the desired server in the tree on the left.
3. Choose *Generate web application* on the context menu or click the corresponding icon.

   Icon for generating a web application for a server

   The *Generate web application* dialog box opens.

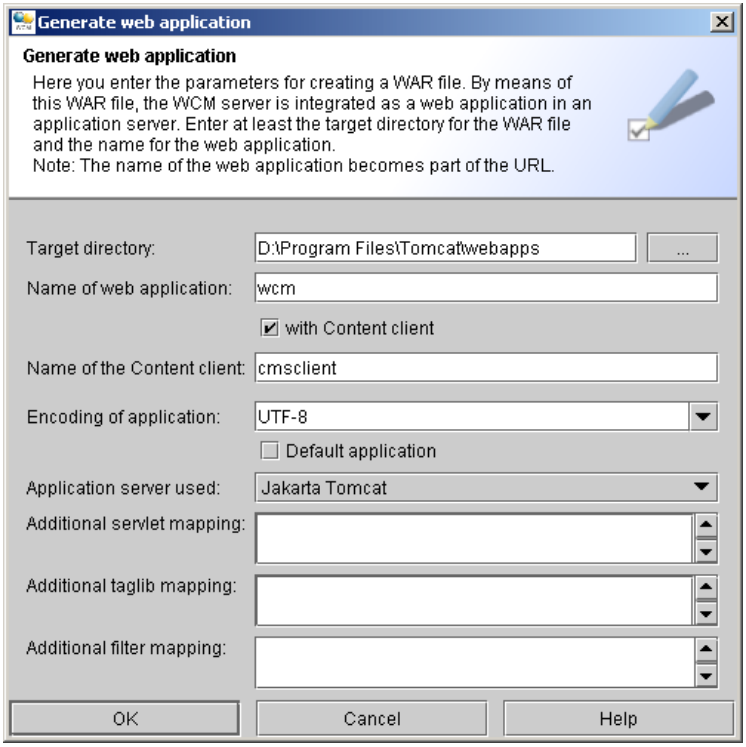

Generate web application
Generate web application
Here you enter the parameters for creating a WAR file. By means of this WAR file, the WCM server is integrated as a web application in an application server. Enter at least the target directory for the WAR file and the name for the web application.
Note: The name of the web application becomes part of the URL.
Target directory:
D:\Program Files\Tomcat\webapps
...
Name of web application:
wcm
with Content client
Name of the Content client:
cmsclient
Encoding of application:
UTF-8
Default application
Application server used:
Jakarta Tomcat
Additional servlet mapping:
Additional taglib mapping:
Additional filter mapping:
OK
Cancel
Help

Fig. 105 – Creating a web application for a server

4. Enter the required information. For detailed information on the individual parameters, refer to the Admin client's online help.

Managing Logged-in Users

Select *System administration* → *Registered users* to get an overview of users who are logged in to the WCM system, e.g. via the Admin client or the Content client.

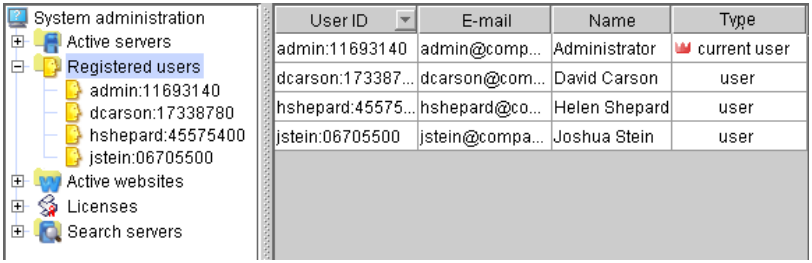


Fig. 106 – List of logged-in users

Information on logged-in users

If you select *System administration* →*Registered users*, the users logged in will be listed in the tree on the left. The table in the right window pane shows the following information:

- complete name of the user
- user ID including session ID
- type of user: “ Administrator” (user with administration rights) or “User” (user without administration rights). The current administrator is marked by the red icon .
- E-mail address

If you select a user in the tree on the left, the detailed user settings are displayed in the right window pane. It is also indicated whether the user is using up a license (see also section “Managing Licenses” starting on page 344).

The ContextList report also offers an overview of the logged-in users.

Logging out users

To log out a user from the system:

1. Select *System administration* → *Registered users*.
2. Mark the desired user in the tree on the left or in the list displayed in the right window pane.
3. Choose *Log out user* on the context menu or click the corresponding icon.

   Icon for logging out a user

4. Confirm the security prompt by clicking the *Yes* button.

Uncompleted actions that the logged-out user has been performing are completely undone by Livelink WCM Server. The user can no longer perform any actions.

> **Note:** For maintenance work on the WCM system, the server run level 4 “Single user mode” is available. When running the server down to this run level, all users, except the active administrator, are automatically logged out (see table “Server run levels” on page 319).

Managing Active Websites

Select *System administration* → *Active websites* to get an overview of the active websites in the WCM system.

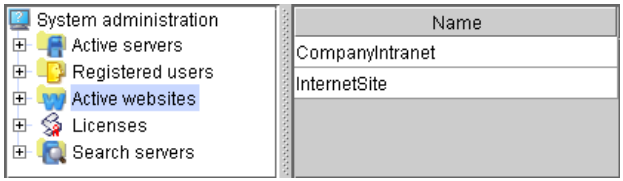


Fig. 107 – Overview of active websites

The following functions are available to you:

- changing the run level of a website (see “Website Run Levels” on page 341)
- overview of the servers on which the website is available (see “Overview of the Assigned Servers of a Website” on page 344)

Website Run Levels

Run levels are a criterion for ranking the execution of certain processes. Run levels exist for servers and for websites. The website run levels are based on the server run levels and are only available if the respective servers are in run level 4 “Single user mode” or 5 “Server up”. If the run level of a server is further reduced, the websites are also shut down automatically.

For an overview of the server run levels, refer to table “Server run levels” on page 319.

The following table explains the run levels of websites.

Table 17 – Website run levels

No.	Name	Description	Required server run level
6	Website inaccessible	One or all websites are no longer accessible (not even for read-only access).	4 “Single user mode” 5 “Server up”
7	Configuring website	The specified website is configured in this run level (the configuration data is written). When changing to the next higher run level, the websites are initialized for read-only access.	
8	Website read only	One or all websites are available for read-only access. When changing to the next higher run level, the deployment systems are initialized.	
9	Deployment complete	Initialization of the deployment systems is complete, i.e. deployment jobs are in progress. On transition to the run level “Website read only”, no more deployment jobs are processed. On transition to the next higher run level, the websites are released for write access.	
10	Website up	One or all websites are available for write access.	4 “Single user mode” 5 “Server up”

The run level of a website must be changed in order to allow changes such as new object types or object categories to take effect. The run level of websites can be changed on a specific server or on all assigned servers.

- Changing the website run level on a specific server:

  Choose *Set website run level* via *System administration* → *Active servers* → *Associated websites* → *{website name}* and select the desired run level.

- Changing the website run level on all servers assigned:

  Choose *Set website run level on all servers* via *System administration*→ *Active websites* → *{website name}* and select the desired run level.

Note: If you change the run level of a website, users should no longer access the website via the Content client. You can get an overview of logged-in users via *System administration* → *Registered users*. You can also log out users here.

Overview of the Assigned Servers of a Website

Select *System administration* → *Active websites* → *{website name}* → *Associated servers* to get an overview of the servers on which the selected website is available.

Fig. 108 – Overview of the servers assigned to a website

In addition to the server names, the current website run level on this server is also displayed.

Managing Licenses

As a result of the license contract with Gauss Interprise AG, you have licensed specific performance features of Livelink WCM Server.

Select *System administration* → *Licenses* to get an overview of the Livelink WCM Server components that are used and available. The display in the right window pane indicates which licenses you have and which ones are currently in use.

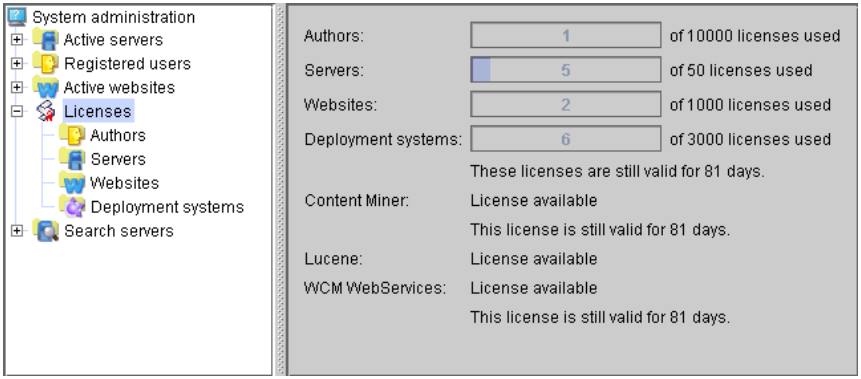


Fig. 109 – License display in the system administration

- *Authors:* the number of concurrent authors. These users are counted from the first write access to WCM objects until they log out. If the number of licensed authors is exceeded, additional users can still log in to the system, but they cannot make or save any changes.

  Every administrator logged in to the Admin client has write access and therefore uses up one license.

  If an author does not log out properly, but does not continue to work in the WCM system, the inactive author session will be terminated after a certain period of time. The time that an author session remains valid (the so-called *Expiration interval*) can be specified in the settings of the Administration server (*Administration* tab).

  If you open the *Users* item, a list of users and session IDs of the logged-in users with write access is displayed.

- *Servers:* number of servers. All WCM server processes in the WCM system are counted, i.e. master Admin server, master Content server, and all proxy servers.

  If you open the *Servers* item, a list of the installed servers is displayed in the right window pane.

- *Websites:* number of websites

  If you open the *Websites* item, a list of the configured websites is displayed in the right window pane.

- *Deployment systems:* number of deployment systems

  If you open the *Deployment systems* item, a list of the installed deployment systems is displayed in the right window pane.

- Installation of additional products of Livelink WCM Server, such as Search servers or WCM WebServices

If you have limited-term licenses, e.g. for test purposes, the remaining validity period is also shown. You can use the utility “License expiration notification” in the configuration to specify who is to be notified before the expiration of limited-term licenses, and when this person is to be notified, see section “Managing Utilities” on page 310.

To prevent misuse of the software, licenses not limited by time are restricted to specific IP address ranges. If you assign new IP addresses from different IP address ranges to your servers, please contact Gauss Interprise AG well in advance to obtain license keys that are valid for the changed IP addresses.

During installation, you specify the path to the license file that you received from Gauss Interprise AG. You can also use the installation program to update your license (see Livelink WCM Server Installation Manual).

Data Backup

For security reasons, the data of the WCM system must be archived at regular intervals. The following data should be backed up:

- the databases of the RDBMS in which WCM objects, deployment information, and (optionally) user information are saved. See “Backing Up the Database” on page 348.
- the complete WCM installation directory. The configuration files in XML format are particularly important. See “Backing Up the WCM Configuration” on page 349.
- optional: the files in the directories of the deployment systems. By default, the files generated by the deployment systems are saved in the subdirectories **{WCM installation directory}\website**. The generated files must not necessarily be backed up, as they are regenerated during the next deployment of the WCM objects. You can use the deployment agent supplied with the product for this purpose, see “ManualDeployment” on page 294.
- the configuration files of the web server used (or of the HTTP server and the JSP engine) as well as JavaBeans, servlets, or tag libraries that are integrated in the class path of the web server

Notes

- The actual data backup is not performed with Livelink WCM Server. For this purpose, external programs for backing up databases and file systems are used. These programs are not supplied with Livelink WCM Server.

- The exact procedure for performing a backup strongly depends on the RDBMS you use. The IT infrastructure of your company also plays a decisive role. For this reason, there is no generally valid backup concept. This section describes which components of the WCM system must be backed up and explains the general procedure for backing up a WCM system.
- If errors occur while the system is being backed up, they will not be evaluated by the WCM system. The system administrator is responsible for performing the data backup successfully.
- Gauss Interprise AG would be pleased to help you work out a backup concept for your WCM system. Please contact Professional Services.

Backing Up the Database

Depending on the RDBMS used and its backup mechanisms, it might be necessary to set down the run level of the website and/or the servers for the backup:

- If the RDBMS runs in the logging mode, an online backup can be performed. In this case, the websites should be run down to run level 8 “Website read only” for ensuring a consistent state of the website data.
- If an offline backup is performed, the connections from the database to the master Content server or to the master Admin server (if the user data is managed in the RDBMS) will be interrupted during the backup. To avoid error messages of the servers, the servers should be shut down completely before an offline backup.

The frequency of the data backup depends on how often your website and user data is changed.

Note: The database and the WCM configuration files are usually backed up separately. However, these two backups must be synchronized so that the status of the database corresponds to the status of the configuration files. For example, when creating websites, changes are made to both the database and the configuration files. Restoring different backup statuses might lead to inconsistencies in the WCM system.

If you use a distributed WCM system with separate data storages, you can also back up the data stored there. It is, however, possible to repair proxy data storages by means of the “DatabaseUpdate” agent. If a proxy data storage fails, the data can be restored by means of the master data storage. See “DatabaseUpdate” on page 292.

Tip: Export the WCM-managed websites at regular intervals and save the export files. In the case of errors in the master Content server of the website, this makes it possible to restore the website data after reinstalling the WCM system. For information on exporting and importing websites, refer to section “Exporting and Importing Websites” starting on page 246.

Backing Up the WCM Configuration

The configuration of the WCM system is saved in XML files in the WCM installation directory. You should back up the entire WCM installation directory at regular intervals. The frequency depends on how often you change the configuration of the WCM system (e.g. add or assign agents, assign proxy servers, create websites, or edit administration rights). The backup of the configuration files must be synchronized with the database backup.

During the data backup, no configuration changes must be made.

Restoring Backed-up Data

To restore a WCM system from a backup:

1. Shut down the servers completely.
2. Replace all files in the WCM installation directory with the corresponding files from the backup copy.
3. Restore the backup of the database.
4. Restart the servers.
5. If necessary, restore the proxy data storages by means of the “DatabaseUpdate” agent (see “DatabaseUpdate” on page 292).
6. Use the deployment agent supplied to let all WCM objects be processed by the deployment (see “ManualDeployment” on page 294).

   You can now continue to work with the WCM system, which reflects the status of the restored backup copy.

CHAPTER 11
System Overview

The *System overview* view provides an overview of the structure and components of your WCM system. The data is displayed in clearly arranged overviews so that you can see the various components at a glance. These include, for example, the computers hosting the WCM servers, the connections between the servers and to the database (or to the LDAP directory service), as well as information on web servers and firewalls.

The information on the WCM system can be saved as an XML file and sent, for example, by e-mail to the Technical Support at Gauss Interprise AG. The system overview also allows you to read the configuration of another WCM system from an XML file and display it in graphical overviews.

To open the system overview, click the

tab in the Admin client.

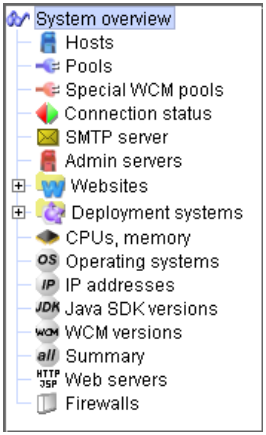


Fig. 110 – The system overview items

A tree-like view displays the items of the WCM system on which information is available, see section “Information in the System Overview” starting on page 354.

By means of the system overview functions available via the context menu or the toolbar, you can write the data retrieved for the WCM system to an XML file, send system files by e-mail, or check the data for plausibility. See section “Functions of the System Overview” starting on page 358.

Information in the System Overview

When you select one of the items in the tree, the associated data is retrieved and displayed in a graphical overview in the right window pane. The components of the WCM system are displayed on the basis of the computers on which the components are installed.

When calling the system overview for the first time after starting the Admin client, the current data is retrieved from the WCM system. However, the overview will not be updated automatically to avoid time-consuming load processes in the case of large systems. To display the current status, e.g. after configuration changes, use the command *Read data from WCM system* from the context menu or click the appropriate icon in the toolbar. Afterwards, refresh the view.

Icon for reading the data from the WCM system

Icon for refreshing the view

Above each overview in the right window pane, a legend explains which components are displayed in what color. If you can perform functions in the selected view, this is also indicated.

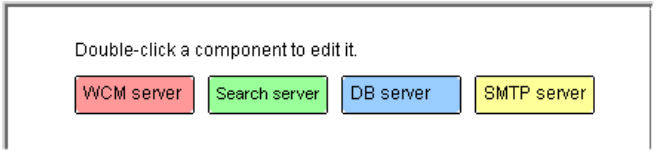


Fig. 111 – Legend in system overview

The following table provides a brief overview of the individual items of the system overview. For detailed information on the individual items, refer to the Admin client's online help.

Table 18 – System overview items

Item	Available information
Hosts	Shows the computers hosting the various WCM servers, the Search servers, the RDBMS, the LDAP servers, and the SMTP server used. If you have entered information on the web server or a firewall via *System overview* → *Web servers* or *Firewalls*, this information will also be displayed.
Pools	Shows the pools configured for the connections between the WCM servers, to the RDBMS, and to the LDAP directory service (if used), including all ports used
Special WCM pools	Shows the configured special WCM pools for connections between two servers, including the ports used
Connection status	Status of the connections in the configured pools Connections that cannot be established at the moment (e.g. because the respective server is not running) are marked by red arrows. Active connections are represented by a green arrow.
SMTP server	Shows the connections from the WCM servers to the SMTP server, including the ports used
Admin servers	Shows the assignments between Content servers and responsible Admin servers and between Search servers and Content servers
Websites	After selecting a website: Shows the master Content server and the assigned proxy Content servers, including the routing between the servers and the database connections
Deployment systems	After selecting a website: shows the deployment systems installed on the assigned Content servers, including routing between the servers and the database connections

Item	Available information
CPUs, memory	In this overview, you can enter the number of CPUs, the speed, and the memory size for each host computer.
Operating systems	In this overview, you can enter the operating system used for each host computer (if it has not been retrieved automatically).
IP addresses	In this overview, you can enter the IP address for each host computer (if it has not been retrieved automatically).
Java SDK versions	Shows the versions of the Java SDK or Livelink WCM Server used, including patch level These values are retrieved automatically by the system when the servers start.
WCM versions	
Summary	Summary of the information regarding *Operating systems*, *IP addresses*, *Java SDK versions*, and *WCM versions*
Web servers	In this overview, you can enter the data of the web server installed on the hosts. You can also enter the path to configuration files to be included in the collection of system data. For collecting the system data, click the *Send system files* button.
Firewalls	In this overview, you can enter for the respective hosts whether they are protected by a firewall. For each firewall entered, the incoming and outgoing connections are displayed.

Functions of the System Overview

The system overview offers you various functions for reading the data of your own or another WCM system, saving the data, or sending it by e-mail (e.g. to the Technical Support at Gauss Interprise AG).

> **Note:** Before sending information to the Technical Support, use the *Verification* function to check whether the data is complete and plausible.

The functions are called via the toolbar. The individual icons offer the following functions.

Table 19 – Icons and functions in the *System overview*

Icon	Function in system overview
	Read data from WCM system: reads the configuration of the WCM system To avoid time-consuming load processes, the display of the system overview is not refreshed automatically. Use this icon to get an up-to-date overview of your WCM system, e.g. after configuration changes.
	Read data from XML file: reads the configuration of a WCM system from an XML file You can use this function to get an overview of another WCM system or an earlier status of your WCM system, which was saved by means of the function *Write to XML file*. After the XML file has been read, the windows of the system overview show the data as it is stored in the XML file.
	Write to XML file: saves the data of the system overview in an XML file You can use this function to save the current data of the system overview in an XML file. You can, for example, send this file to the Technical Support of Gauss Interprise AG or archive it.

Icon	Function in system overview
	Send system files: sends the data of the system overview by e-mail See the following section
	Verification: checks whether the data of the system overview is complete and plausible The results are displayed in a dialog box. The check is performed automatically before the system files are sent by e-mail.
	Update element data The data of the system overview is not retrieved again when updating the element data. For this purpose, use the function *Read data from WCM system*.

Sending System Files

Use this function to collect the system data in an archive. You can send this archive by e-mail to Technical Support of Gauss Interprise AG. The archive has the following content:

- the current data of the system overview
- the content of some subdirectories of the WCM installation directory
- the reports and logs of the WCM servers
- hardware information on the computers hosting the WCM servers

  The hardware information included in the archive can be determined via *System overview* → *CPUs, memory*.
- the log and configuration files of web servers/application servers

  To specify the log and configuration files contained in the archive, select *System overview* → *Web servers*. In the parameters of the web server, you can specify the paths to the respective files.

Notes:

Always enter the complete path to the file including the file name.

You can specify several log and configuration files for the archive. Confirm the path by pressing ENTER. Enter the next path in the new line.

Prerequisites for Sending Data

For the information on the web servers and hardware used to be included in the archive, you must enter this information in the system overview. Also, the e-mail settings in the Admin client must be configured correctly.

Entering information in the system overview

Please enter the following information:

- CPUs, speed, and memory of the computers hosting the WCM servers
- information on the HTTP servers, JSP engines, or application servers used, and paths to the respective configuration files

Notes:

For the log and configuration files of the web server used to be included in the system data, the user who started the WCM server must have access rights for the respective computers and directories in which the log and configuration files of the web server are located.

To ensure that the information on hardware and web servers is saved centrally, you should enter the respective data by means of an Admin client that accesses the master Admin server. This Admin client must not necessarily be installed on the computer of the master Admin server.

Settings of the SMTP server

The e-mail to Technical Support is sent via the Administration server. In the settings of all WCM servers, the SMTP server must be configured correctly. To configure the SMTP server, select *Configuration* → *Servers* → *{server name}* → *Miscellaneous* tab.

Regarding the SMTP server used, the following additional requirements must be met:

- The SMTP server must be able to send e-mails to external domains.
- The SMTP server must identify and accept the mail sender specified in the Admin client as a valid address.
- Please also consider restrictions regarding e-mail size in the local SMTP server.

Generating E-Mail with System Files

To generate an e-mail with the system files:

1. Click the *Send system files* icon.

   The *Generate e-mail with system files* dialog box opens.

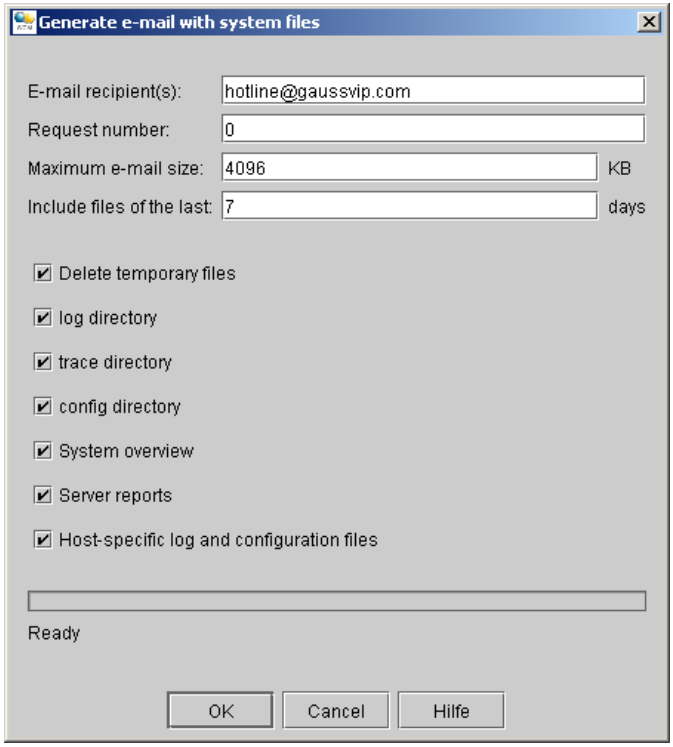


Fig. 112 – Generating e-mail with system files

2. Make the desired entries for collecting the system files. For detailed information on the individual parameters, refer to the Admin client's online help.
3. Click the *OK* button.

   The files are collected in an archive and sent by e-mail to the specified address.

Notes:

The collected archive is meant to be used exclusively by Technical Support of Gauss Interprise AG. It cannot be used as a backup of the system files. For general information on backing up the WCM system, refer to section “Data Backup” on page 347.

If sending the system files is not possible, switch on the trace log for the class `de.gauss.vip.service.hotmailservice` for the Administration server (see “Trace Logs” on page 332). Afterwards, try again to send the system files and send the trace log to Technical Support of Gauss Interprise AG. Then, switch off tracing.

Glossary

Access control list – For each WCM object, users, groups, roles, and group-roles that have access to this object can be specified. The individual access rights are specified separately for each principal authorized to access the object. Also called ACL.

ACL – Access Control List

Address – see *URL*

API – Application Programming Interface. Livelink WCM Server offers various APIs to access the functionalities of the WCM servers: the WCM Java API, the remote API, the Portal Manager API, and WCM WebServices.

Applet – Java program embedded in a website. An applet is loaded by the server and executed by the client.

Application server – Also enterprise application server. An infrastructure that acts as middleware and/or development and runtime environment for web applications and wireless applications. An application server interacts with the API (Application Programming Interface). Thus, more flexibility is offered and high-level tasks can be performed remotely or via the Internet.

This allows a user at a web page to perform more sophisticated server interactions, such as querying a database or running other programs loaded on that server. Application servers often offer additional security features, load balancing, and failover mechanisms as well as scaling functions and interaction functions.

ASP – Active Server Pages. HTML files with specifically identified embedded JavaScript or Visual Basic Script programs that are run on the web server. The result is then sent to the client in normal HTML format.

Attributes – Special metadata that can be defined differently for each object type. Attributes are grouped in attribute sets.

Attribute set – Set of attributes. Attribute sets can be combined with object types. In this way, all WCM objects that are created on the basis of this object type can be equipped with the attributes of the assigned attribute set. Attribute sets are edited in the Admin client or in the Content client.

Cache – Temporary storage between slow and fast units that saves frequently used data. A cache is used to reduce the access time.

CGI – Common Gateway Interface. A web server interface used to run scripts or programs that generate user responses on HTML forms. CGI programs are usually located in a special directory on the HTTP server. Special URLs call such a CGI program, which in turn generates an HTML response to the request and sends it to the client.

Context ID – Object that is assigned to a user after successfully logging in to the WCM system. A context ID is always unique throughout the entire system. It thus precisely identifies a user. If a context ID is not used over a certain period of time, it expires.

Database – Structured data stock of related content that is managed by a database management system.

DBMS – Database management system. A DBMS permits controlled access to databases and their management.

Deployment – Deployment is the distribution of data. The deployment of Livelink WCM Server performs two main tasks: first, generating pages from the WCM objects stored in the database and distributing the generated files to the appropriate directories; second, notifying the WCM servers of changes in the WCM system.

Deployment system – The deployment systems generate pages from the WCM objects and distribute the generated files to the appropriate directories. From there, the files become visible for the users via an HTTP server. Deployment systems may be of various types and categories.

Deployment system category – Depending on the way of processing deployment jobs, deployment systems are assigned to various categories: *Standard deployment systems* automatically generate a new page every time a WCM object is changed. The generated pages are stored in the file system. *Dynamic deployment systems* generate the pages on the basis of user-defined settings and only when the page is requested via the HTTP server. The generated files are stored in a flat file structure. By means of *Search engine deployment systems*, you can prepare your website data for use with a search engine. *WebDAV deployment systems* are required for the use of WebDAV clients. *InSite Editing deployment systems* provide the basis for editing and adding content directly in the website – without the Content client.

Deployment system types – On the basis of the staging concept of Livelink WCM Server, a distinction is made between deployment systems of type “Edit”, “QA”, and “Production”. Different views of the website data are generated, depending on the type.

Edit view – In the Edit view of Livelink WCM Server, the objects of a website are created and edited. Here the most current status of the objects is visible.

Extranet – Information platform based on Internet technology for business communication with authorized external users, e.g. partners or customers.

Firewall – Hardware or software that monitors the data flow between a public and a private network and protects networks against unauthorized access. Livelink WCM Server supports architectures protected by firewalls.

Form – Possibility to integrate dialog elements to be filled in by users in web pages. The content of such a form can be sent to the server for further processing.

Frame object – Object type for a frameset

Frame topic – Frame object that is at the same time used as a topic (for content organization). See also *Topic*.

Group – Collection of users for which specific access rights can be defined. User groups are usually tied to organizational units, such as departments and projects.

Group-role – Combination of a group and role. The group-role is not an organizational unit that is defined in the Admin client, but a configuration option for the object access rights in the Content client.

HTTP – Hypertext Transfer Protocol. A communication protocol for transferring HTML pages

HTTP server – An HTTP server offers an HTTP client (browser) HTTP services over a standardized TCP/IP port.

HTTP tunneling – When HTTP tunneling is used, the data in a WCM system is sent wrapped in a HTTP data flow. The data is coded according to the VIPP protocol and additionally packaged in HTTP.

In firewall scenarios, HTTP tunneling is a common transfer method. Firewall systems interpret the data flow and, among other things, enable only certain protocols. If the VIPP protocol is not enabled, the data can be transmitted by means of HTTP tunneling.

Java – Object-oriented programming language developed by Sun Microsystems and used especially in the field of Internet technology. Security aspects and platform independence are the basic philosophies of Java.

Java 2 SDK – Java 2 Software Development Kit. The SDK contains all components that are required for creating and using programs and applets in Java, i.e. the Java compiler, the Java Runtime Environment, and several utilities.

JavaScript – Scripting language for integrating executable scripts in HTML pages. JavaScript can be used to incorporate plausibility checks and calculation functions in forms.

JDBC – Java Database Connectivity. A mechanism of communicating with existing databases. Drivers form the interface between the Java program and the database.

JRE – Java Runtime Environment. The JRE contains all components required for running Java programs, i.e. the Java Virtual Machine and the Java Class Library.

JSP – JavaServer-Pages. HTML files with specifically identified embedded Java programs that are converted into servlets by using the JSP engine and then executed on the web server. The result is then sent to the client in normal HTML format (without Java).

JVM – Java Virtual Machine. The JVM makes it possible to run platform-independent Java programs on a specific computer. It is part of the JDK or JRE.

LDAP – Lightweight Directory Access Protocol. The LDAP is based on the X.500 standard and is supported by most major software manufacturers. LDAP directory services are used to manage user information.

Master server – Only master servers have read and write access to the data of a WCM system. The master Content server manages website data, while the master Administration server manages the configuration and system data of the WCM system. See also *Server category*.

Metadata – Every WCM object has a number of object information assigned to it (e.g. expiration date, language). These are known as metadata.

Object category – Assignment of a WCM object to a specific category. Due to this assignment, the WCM object has a set of additional special attributes (metadata).

Object type – The specific kind of object, e.g. “HTML page”, “HTML template”, “Topic”. Various properties of the WCM object result from the object type. The object type is defined when the object is created. There

are only a few cases in which it may subsequently be changed. Object types can be edited in the Admin client or the Content client.

Pool – The different connections within a WCM system are managed in pools. These include, for example, connections for communication with an LDAP directory service or for communication between the WCM servers. If a connection is required, it is taken from the respective pool. After the data transfer, the connection is returned to the pool. Pools always combine connections of the same type, e.g. connections to databases (JDBC pools) or connections between WCM servers (WCM pools).

Portal – A portal is a website that serves the user as a central point of access – as a gate – to certain Internet services. A portal often offers topic-specific and personalized offers and information.

Production view – The Production view of Livelink WCM Server makes the released pages of a website available to the user. By means of a web server, these pages can be accessed in the Internet, intranet, or extranet.

Proxy server – A proxy server is used to intercept requests from a client application, e.g. a browser, to one or more other servers. If the proxy server can meet the request, it sends the requested data back to the client. Otherwise, it forwards the request to the specified server.

In the context of Livelink WCM Server, WCM servers of the category “proxy” do not have write access, but only read access to the WCM objects or the configuration. Changes to the WCM objects are only possible via the master Content server, changes to the configuration of the WCM system are made only via the master Administration server. See also *Server category*.

QA view – The QA view of Livelink WCM Server is used for quality assurance of the objects and thus of the website content. This view thus performs the control function between editing in the Edit view and publication in the Production view.

RDBMS – Relational database management system. A DBMS in which relations between data records from individual databases can be used. In

contrast to an RDBMS, there are also object-oriented and object-relational DBMS.

Relator – Due to the integration of web content management and Livelink, you can add Livelink objects as WCM objects in a WCM-managed website. These WCM objects are called relators. They always refer to a certain version of a Livelink object. For integrating a single Livelink object, the WCM system provides the object type “Livelink relator”. For integrating Livelink folders, the WCM object type “Livelink folder relator” is provided.

Role – Collection of users, similar to a user group, for which specific access rights can be defined. The user role is usually defined in terms of tasks, whereas user groups are generally tied to organizational units, such as departments or projects.

Search server – The combination of Index and Query system in Livelink WCM Server is called “Search server”. Each Search server is assigned to exactly one WCM server. It is, however, possible to assign more than one Search server to a WCM server.

Server category – In a WCM system, a distinction is made between master and proxy servers. Master servers have write access to the data of the WCM system, while proxy servers have only read access. The master Content server manages the website data, the master Administration server manages the configuration and system data. In addition to this, any number of proxy servers can be set up.

Server type – According to the tasks of the servers, there are two server types: Content servers for managing website data and Administration servers for managing the user, configuration, and system data of the WCM system. Basically, every Content server is able to provide all views of the data of the managed websites – Edit, QA, and Production. The available views may be limited by the fact that the Content server only receives the data of certain views.

Servlet – Java program executed by the web server for generating the data requested by a client by means of an HTTP request

SMTP – Simple Mail Transfer Protocol. A protocol for transferring e-mail messages, for example between different servers

SSL – Secure Socket Layer. A protocol layer for the communication between the components of a WCM system that ensures that the data transfer will be secure in terms of eavesdropping and falsification. SSL can be used both for the VIPP protocol and HTTP tunneling.

Statification – During statification, the dynamic components of, for example, a JSP page are converted into static components. The result is pure HTML without Java code.

TCP/IP – Transmission Control Protocol/Internet Protocol. Basic protocol for data transfer in the Internet

Topic – Combination of an HTML page for direct display of information and a list for accommodating subordinate objects. The topics are shown as nodes in the object tree and thus help structure the website.

Type – see *Object type*

URL – Uniform Resource Locator. A unique address in the World Wide Web.

VIPP – VIP Protocol. A proprietary protocol for exchanging data between the components of a WCM system. VIPP can be tunneled in HTTP for communication in WANs or over the Internet.

WCM server – In a WCM system, there are several WCM servers working in parallel (server processes). The exact tasks of a server depend on the server type and server category.

WCM tag – Special element for integrating WCM specific data in an HTML page. WCM tags are used in particular when creating templates.

WebDAV – The WebDAV (Web-based Distributed Authoring and Versioning) protocol supports Internet and group-based working on the basis of standard Internet technologies. Thanks to WebDAV, users do not need a special client for creating WCM objects, jointly editing them, and managing them by means of WevDAV-capable tools.

Web repository – The name given to the area where the WCM system stores and manages all the objects belonging to a website

Web server – Program for processing the requests from a browser. A web server corresponds to an HTTP server that offers additional web services, such as those of a JSP engine.

Web technology – Client/server technology based on TCP/IP. The advantage lies in the open standard, which permits the creation of heterogeneous systems.

Index

A

absolute links
- dynamic deployment system 275
- standard deployment system 275
- WebDAV deployment system 275

access control 65, 131
- administration rights 75
- object rights 72
- orphan objects 243
- Secure Access in general 78
- users, groups, roles in general 67

access rights
- default settings 71
- in general 72

access to Admin client
- groups/roles 147
- users 141
- World 150

AccessController report 326

actions
- cancel 335

actions in progress 334
- cancel 335

active servers 317

active websites 341

add
- attribute set 236
- connection type 168
- converter 242
- deployment system 275
- functional area 152
- group or role 145
- items in general 106
- object category 238
- object type 231
- pool 162
- user 138

Admin client
- as a web application 117
- change display mode 117
- context menu 101
- create web application 119
- delete items 107
- edit assignments 109
- edit item settings 107
- edit items 102
- filter functions 104
- help 128
- in general 95
- introduction 17
- log in and out 95
- menu bar 101
- new items 106
- select Admin server 117
- select functions 100
- select items 103
- settings 116
- start 95, 117
- toolbar 100
- update web application 121
- user interface 98
- views 99

Admin server
- deregister proxy Admin server 195
- in general 32
- information in system overview 356
- manage proxy Admin servers 189
- select for Admin client 117

administration rights
- for import and export of complete websites 248
- for import and export of website subtrees 264
- groups/roles 147

in general 75
users 141
World 150
agents
assign server 184
assign to server 287
automatic conversion 296
ContentMinerNotification 296
DatabaseUpdate 292
DefaultContent 307
delete 288
ExpirationNotification 290
FileLabeling 298
integrate 284
LinkResolving 295
LivelinkFolderSynchronization 302
manage 282
ManualDeployment 294
monitor in system administration 335
parameters 285
ReleaseNotification 290
report in system administration 328
settings 286
start 336
stop 336
supplied agents 288
translate names 123
website export and import 296
API 53
applet
distribute Admin client 118
application server
generate web application 336
architecture
distributed system with two websites 62
firewall 57
minimum system 56
of a WCM system 55
system with separate data storages 60
ASCII encoding
in general 83
assign
agent to server 184, 287
converter to website 240
functional areas to principals 154
orphan objects 243
pool to server 182
server to website 177, 228
user, group, role to website 210
websites to principals 156
assigned servers of website 344
assignments
edit 109
functional areas 154
group 146
information window 114
role 146
servers 174
users 140
websites 156
associated websites 323
attribute sets
assign to object type 232
delete 237
functions 235
manage 234
new 236
settings 236
attributes
edit 236
translate names 123
automatic conversion 296

B

backup 347
database 348
required run level 347

WCM configuration 349
base directory
minimum configuration for new website 211
base URL
minimum configuration for new website 211
basics 25

C

caching
website 209
cancel an action 335
categories of deployment systems 38
class
agent 284, 286
command line mode
export and import of websites 253
communication
error logs 329
communication channels
in general 47
in website settings 226
new website 220
concepts 25
configuration
Admin client 116
backup 349
synchronize of master and proxy Admin 194
ConfigurationManager report 327
connection status
information in system overview 356
connection types
custom 160
default 160
delete 170
functions 160
in general 50
manage 159
new 168
settings 168
translate names 123
ConnectionManager report 327
console
export and import of websites 253
Content client
control functions via functional area 68
in general 16
introduction 16
Content server
in general 32
ContentMiner notification 296
context menu 101
ContextList report 327
conversion
automatic 296
ConvertContent 296
converter 240
configure 242
conversion process 241
delete 243
functions 242
prerequisites 241
settings 242
cookie for Secure Access 81
CPUs
information in system overview 357
create
website 204
create website
application name and directory 214
assign principal 210
base directory and URL 211
deployment systems 216, 222
user-defined 218

D

data backup 347
data storage
  users 45
  website 43
database
  backup 348
  update on proxy Content servers 292
  users 45
  website 43
database clean-up 310
default content 307
default object rights
  in general 71
DefaultContent 307
delete
  agent 288
  attribute sets 237
  connection types 170
  converter 243
  deployment system 278
  functional area 155
  group or role 149
  items in general 107
  object category 240
  object type 233
  pools 167
  servers 197
  user 142
  website 245
deploy resources 122
deployment
  agent for manual deployment 294
  deployment system categories 38
  deployment system types 37
  in general 36
  stop 324
deployment system categories 38
  dynamic 40
  InSite Editing 43
  search engine 42
  standard 39
  WebDAV 42
deployment system types 37
deployment systems
  delete 278
  functions 274
  information in system overview 356
  logs 329
  manage 273
  new 275
  of a website 227
  on a server 180, 327
  settings 276
  user-defined creation of a website 222
deployment tasks 36
DeploymentAdapter report 327
DeplyomentForwardThread report 327
DeplyomentSystemHandler report 327
deregister
  proxy Admin server 195
directory
  minimum configuration for new website 211
DisplacingObjectCache report 327
distribute Admin client
  applet 118
  Java Web Start 119
dynamic deployment 40

E

Edit view 29
e-mail settings
  servers 176
encoding 84, 208
  in general 83
error logs 329

error messages 129
Admin client 129
expiration interval
set 177
ExpirationNotification 290
configure e-mails 290
export
complete websites 247
complete websites (console) 253
logging 268
parameters for subtree export 264
parameters for website export (console) 253
parameters for website export (GUI) 250
website subtrees 258
websites (in general) 246
export-import-conf.xml 253

F

file labeling 298
filter functions 104
firewalls
information in system overview 357
scenario 57
folder
synchronize Livelink folder with WCM system 302
functional areas
assign 154
assign to object type 232
delete 155
in general 68
manage 150
new 152
settings 153
translate names 123
functions
attribute sets 235
connection types 160
converter 242
deployment systems 274
object types 230
pools 161
servers 173
system administration 315
system overview 358
user administration 132
users 136
websites 201

G

global WCM pools 161
in general 52
groups
administration rights 147
assign functional areas 154
assign websites 156
assignments 146
delete 149
in general 67
manage 143
new 145
settings 146
GUI 98

H

help 128
hosts
information in system overview 356
hotline
information from system overview 353
send system files by e-mail 359
HTTP
in general 48

I

icons
change in Admin client 117

import
complete websites 247
complete websites (console) 253
logging 268
parameters for subtree import 264
parameters for website import (console) 253
parameters for website import (GUI) 252
website subtrees 258
websites (in general) 246
information
for Technical Support 353
on Admin server (login) 97
on assignments of an item 114
on logged-in users 339
on the WCM system 354
InSite Editing
in general 43
integrate
agent 284
internationalization 123
introduction 15
IP address
information in system overview 357
ISO-8859-1
in general 83
items
delete 107
edit 107

J

Java API 53
Java SDK
information in system overview 357
Java Web Start
distribute Admin client 119
Java Webstart
<Italic>see Java Web Start
JDBC pools 160
for website 208
new website 219

K

keyboard shortcuts 102

L

language
for root object of new website 209
Latin-1 encoding
in general 83
LDAP
new pool for additional LDAP servers 163
set WCM attributes 134
LDAP pools 160
LDAP user administration
in general 45
license expiration notification 310
LicenseManager report 327
licenses
LicenseManager report 327
monitor 344
link format 275
Livelink
agent for folder synchronization 302
connection type for pools 160
new pool for Livelink system 162
Livelink pools 160, 161
Livelink user administration
in general 45
Livelink WCM Server
configuration for UTF-8 (overview) 84
introduction 15
server concept 32
staging 29
Unicode 82

workflow 30
LivelinkFolderSynchronization 302
LivelinkObjectHandler report 328
LivelinkSystemManager report 328
localization 123
log in and out of the Admin client 95
log out
user 340
logged-in users
information 339
monitor 339
overview in ContextList report 327
login 95
login information 97
logs 329
Admin client 129
deployment 329
WCM servers 329
Look and feel for Admin client 117

M

maintenance 320
manage
active servers 317
active websites 341
agents 282
attribute sets 234
deployment systems 273
functional areas 150
groups and roles 143
licenses 344
logged-in users 339
object categories 237
object types 229
other WCM products 115
pools and connection types 159
server agents 282
servers 173
users 136
utilities 310
websites 201
manual deployment 294
mark items 103
master Administration server
in general 33
master Content server
in general 33
website 208
match
configuration of master and proxy Admin 194
Livelink folder with WCM system 302
memory
information in system overview 357
menu bar 101
minimum configuration
website 207
minimum system
architecture 56
monitor
active servers 317
multiple data storages
scenario 60

N

name
agent 284
deployment system 216
website 207
new
attribute set 236
connection type 168
converter 242
deployment system 275
functional area 152
group or role 145
object category 238
object type 231
pools 162

users 138
website 204
new items 106

O

object categories
delete 240
manage 237
new 238
settings 239
object rights
default settings 71
in general 72
object types
delete 233
functions 230
manage 229
new 231
settings 231
translate names 123
ObjectManagerImpl report 328
online help 128
operating systems
information in system overview 357
orphan objects
assign 243
overview
of logged-in users 327, 339
overview of WCM system 353

P

parameters
export of websites (GUI) 250
import and export of website subtrees 264
import and export of websites (console) 253
import of websites (GUI) 252
server agent 285
path
Secure Access 186
PoolManager report 328
pools
assign server 182
default pools 161
delete 167
functions 161
global WCM pools 161
in general 50
information in system overview 356
JDBC pools 161
LDAP pools 161
Livelink pools 161
manage 159
new 162
PoolManager report 328
settings 164
special WCM pools 163
Portal Manager API 53
prerequisites
import and export of website subtrees 264
import and export of websites 248
Production view 29
products of Livelink WCM Server 115
programming interfaces 53
property
edit 238
translate names 123
protocols for communication 48
proxy Admin server 189
deregister 195
register 192
select for Admin client 117
synchronize configuration with master 194
proxy Content servers
database update 292
for new website (user-defined

setup) 218
in general 33
website assignment 177, 228

Q

QA view 29

R

RDBMS
backup 348
new JDBC pool 162
ReceiverManager report 328
references
resolve 295
register a proxy Admin server 192
registered users
information 339
manage 339
relative links
standard deployment system 275
WebDAV deployment system 275
release control 310
configure e-mails 310
ReleaseNotification 290
configure e-mails 290
remote API
enable 176
remove
proxy Admin server 195
servers 197
reports 325
AccessController 326
ConfigurationManager 327
ConnectionManager 327
ContextList 327
DeploymentAdapter 327
DeploymentForwardThread 327
DeplyomentSystemHandler 327
DisplacingObjectCache 327
LicenseManager 327
LivelinkObjectHandler 328
LivelinkSystemManager 328
ObjectManagerImpl 328
PoolManager 328
ReceiverManager 328
RunlevelManager 328
save 326
send by e-mail 326
ServerAgentManager 328
ServerInfo 328
ThreadManager 328
update 326
VersionSupervisor 329
resolve references
dynamic deployment system 275
standard deployment system 275
WebDAV deployment system 275
resources
deploy 122
reusability 18
risk management 19
roles
administration rights 147
assign functional areas 154
assign websites 156
assignments 146
delete 149
in general 67
manage 143
new 145
settings 146
root object
language 209
routing
during website setup 220
in general 47
in website settings 226
run level
automatic check 176
for backup 347
of servers 318

of websites 341
RunlevelManager report 328
RunlevelManager report 328
running actions 334

S

scenarios for WCM systems 55
firewall 57
minimum system 56
separate database 60
two websites 62
search engine deployment system 42
Search server notification 296
Search servers
logs 329
Secure Access
in general 78
in server settings 177
manage paths 186
select items in Admin client 103
sender for e-mails 176
separate data storage
scenario 60
server agents
assign to server 287
AutomaticConversion 296
ContentMiner notification 296
DatabaseUpdate 292
DefaultContent 307
delete 288
ExpirationNotification 290
FileLabeling 298
integrate 284
LinkResolving 295
LivelinkFolderSynchronization 302
manage 282
ManualDeployment 294
parameters 285
ReleaseNotification 290
report in system administration 328
settings 286
supplied agents 288
website export and import 296
server categories 33
server concept 32
server logs 329
delete 331
save 331
send by e-mail 331
update view 331
server types 32
ServerAgentManager report 328
ServerInfo report 328
server-relative links
dynamic deployment system 275
standard deployment system 275
servers
actions in progress 334
active website 323
assign agents 184
assign pool 182
assigned to website 177, 228
delete 197
deployment systems 180, 327
for e-mails 176
generate web application 336
manage 173
monitor assigned agents 335
monitor assignment to websites 344
monitor in system administration 317
paths for Secure Access 186
reports 325
routing 47
run levels 318
services 186
settings 176
trace logs 332
types 32
service packs
deploy 122

services
of a server 186
set run level
of websites 324
settings
Admin client 116
agent 286
attribute set 236
connection type 168
converter 242
deployment systems 276
functional areas 153
group or role 146
object categories 239
object type 231
of items in general 107
pools 164
servers 176
users 139
website 226
several websites
scenario 62
shortcuts 102
single sign-on 81
single user mode 320
skins for Admin client 117
SMTP server
information in system overview 356
special WCM pools
add 163
in general 52
information in system overview 356
SSL
in general 48
staging 29
standard deployment system 39
start
Admin client 117
agent 336
status of connections
information in system overview 356
stop
agents 336
synchronization
configuration of master and proxy Admin 194
with Livelink folders 302
system administration 315
functions 315
system architecture 25
system overview 353
functions 358
information 354
send system files 359
system with firewall
scenario 57
system-wide login 81

T

tab
Configuration 99
System administration 99
System overview 99
User administration 99
Technical Support
information from system overview 353
send system files by e-mail 359
template for object content 307
ThreadManager report 328
threads 310, 328
toolbar 100
trace logs 332
delete 334
save 334
send by e-mail 334
update 334
tracing 332

translate items 123
types of deployment systems 37

U

Unicode
configuration of Livelink WCM Server (overview) 84
for website 208
in general 82
update
report 326
server log 331
trace log 334
up-to-date content 18
URL
minimum configuration for new website 211
URL cache invalidation 310
user administration 131
functions 132
in general 45
LDAP 134
user interface of the Admin client 98
user-defined creation of a website 218
users
actions in progress 334
administration rights 141
assign functional areas 154
assign websites 156
assignments 140
delete 142
in general 67
information on logged-in users 339
log out 340
manage 136
monitor logged-in users 339
monitor logged-in users (ContextList) 327
new 138
settings 139
UTF-8
configuration of Livelink WCM Server (overview) 84
for website 208
in general 83
utilities
manage 310
report in system administration 328

V

versions of Livelink WCM Server
information in system overview 357
VersionSupervisor report 329
view
change in Admin client 117
Configuration 99
four views in the Admin client 99
System administration 99
System overview 99
User administration 99
views of the data storage 29
VipDAVApplication 92
VipDAVLockRepository 88
VIPP
in general 48

W

WAR file
generate 336
WCM attributes
set in LDAP 134
WCM configuration
backup 349
WCM Java API 53
WCM pools 160
global 52, 161
special 52, 163
WCM servers
actions in progress 334

assign agent 184
assign pool 182
assigned to websites 177, 228
associated websites 323
delete 197
deployment systems 180, 327
generate web application 336
logs 329
manage 173
monitor assigned agents 335
monitor assignment to websites 344
monitor in system administration 317
paths for Secure Access 186
reports 325
run levels 318
services 186
settings 176
trace logs 332

WCM system
information in system overview 354
scenario 55

WCM versions
information in system overview 357

WCM WebServices 53

web application
create for Admin client 119
for Admin client 117
generate for WCM server 336
update for Admin client 121

web server
information in system overview 357

WebDAV 87

WebDAV client
conversion of objects 296

WebDAV deployment system 42

WebServices 53

websites
assign 156
assign converter 240
assign server 177, 228
available deployment systems 227
caching 209
create with option minimum or minimum (dynamic) 207
delete 245
functions 201
import and export 246
import and export complete websites 247
import and export website subtrees 258
information in system overview 356
language of the root object 209
manage 201
manage active websites 341
monitor assigned servers 344
new 204
object types 229
overview of websites on a server 323
run level 341
set run level on a server 324
set to Unicode (UTF-8) 208
settings 226

Webstart
<Italic>see Java Web Start

workflow 30

World
administration rights 150